TAGnology RFID GmbH | Grazer Vorstadt 142 | 8570 Voitsberg | AUSTRIA
phone: +43 (0)3142/ 28 9 28-10 | fax: +43 (0)3142/ 28 9 28-20 | office@tagnology.com | www.tagnology.com

HF Dual ISO RFID Reader

USER MANUAL

© 2008 HID Global Corporation. All rights reserved.

1502-USM-00-0-02

Firmware Version 2.4

November 4, 2008

Doc Number: 1502-USM-00, Rev A.0

Warning - Read before start-up!

- The product may only be used for the intended purpose designed by for the manufacturer. The operation manual should be conveniently kept available at all times for each user.
- Unauthorized changes that have not been sold or recommended by the manufacturer may have a negative influence on the system the program has been installed or copied on. Such unauthorized measures shall exclude any liability by the manufacturer.
- The liability-prescriptions of the manufacturer in the issue valid at the time of purchase are valid for the device. The manufacturer shall not be held legally responsible for inaccuracies, errors, or omissions in the manual or automatically set parameters for a device or for an incorrect application of a device.
- Only qualified personnel should carry out installation, operation, and maintenance procedures.
- Use of the program and its installation must be in accordance with national legal requirements.
- When working on devices the valid safety regulations must be observed.
- International copyrights are applicable to this program. Unauthorized copying, distribution or resale of this program or of parts of this program is a violation of applicable laws and will be prosecuted.

© 2008 HID Global Corporation. All rights reserved.

Read Me First

About This Guide

This manual describes the HF Dual ISO Reader. Its goal is to describe the reader, how it works, how to integrate it and how to use it.

Contacts

Europe, Middle East and Africa

HID Global Corporation, Ltd. (Haverhill, UK)
email: eusupport@hidglobal.com
main: +44 (0) 1440 714 850
support: +44 (0) 1440 711 822
fax: +44 (0) 1440 714 840

© 2008 HID Global Corporation. All rights reserved.

Contents

Warning - Read before start-up! 2

Read Me First 3

Scope 6

Extended Documentation 6

Overview 7

1 The MIFARE® Transponder Family 10

2 ISO 14443 Type B 16

3 Hardware 18

4 Software 24

5 Frequently Asked Questions 78

References 82

Appendix A - Antenna 82

Appendix B - SAM 82

Appendix C - Short Range Plug & Play Module (RDHS-0404N0-03) 83

Appendix D - Timings 85

Appendix E - Release Notes 87

Appendix F - Approvals / Certificates 89

List of Figures

Figure 1 MIFARE® Standard: sector diagram 10
Figure 2 MIFARE® Standard: sector 0 / block 0 10
Figure 3 MIFARE® Standard: block 3, 7, 11, 15, … 10
Figure 4 State diagram 11
Figure 5 DESFire Memory 13
Figure 6 DESFire state diagram 14
Figure 7 Time slot formula 43
Figure 8 Time slotted answers diagram 43

© 2008 HID Global Corporation. All rights reserved.

List of Tables

Table 1 MIFARE® 4k sector index table 12
Table 2 ASCII protocol frame 24
Table 3 Binary Frame Version 1 24
Table 4 Binary Frame Version 2 24
Table 5 Protocol configuration register 28
Table 6 ISO 14443 A Extended Serial number of part 3 selection 29
Table 7 ISO 14443 A Extended Serial number of part 4 selection 29
Table 8 ISO 14443 A tag type 29
Table 9 ISO 14443 B Extended Serial number of part 3 selection 29
Table 10 ISO 14443 B Extended Serial number of part 4 selection 29
Table 11 Baud rate register 30
Table 12 Baud rate settings 30
Table 13 Exact baud rates 30
Table 14 Communication settings 31
Table 15 Operation mode register 31
Table 16 Protocol configuration register 34
Table 17 Protocol configuration register 34
Table 18 Command overview 35
Table 19 DESFire Command Set 36
Table 20 Error codes 37
Table 21 Baud Rate Values 46
Table 22 Frame Size 46
Table 23 Baud Rate values 47
Table 24 Frame Size 47
Table 25 Flag Type with corresponding flag 53
Table 26 Register Type with corresponding register 54
Table 27 Read USER port return values 58
Table 28 Write User port settings 58
Table 29 Sending Serial Data Frame 58
Table 30 Receiving Serial Data Frame 59
Table 31 Using a MIFARE® card 80
Table 32 Timings 85

© 2008 HID Global Corporation. All rights reserved.

Scope

The HF Dual ISO Reader Module supports a broad range of tags compliant with ISO 14443 type A and B standards, including SR176 tags and tags that belong to the Philips MIFARE® family. An open command structure allows the device to communicate with tags that use an operating system. The read/write unit supports automatic chaining; 256 byte buffer and frame length, extended time framing and up to 848kBaud transmission rates over the air interface.

Additionally this unit implements a DES cipher that enables to use MIFARE® DESFire tags. These tags are designed for use in high security algorithms.

A SAM interface is also available.

Major applications are:

- Access control, identification using high security cards
- Ticketing using standard MIFARE® cards
- Data storage
- Multi-applications using operating systems

Extended Documentation

Please note that all confidential material is excluded from this documentation in order to comply with NDA requirements of our suppliers as well as prevention from unauthorized copies of the reader modules for increasing the security in the applications.

You can obtain the extended documentation containing the confidential information after signing a NDA.

© 2008 HID Global Corporation. All rights reserved.

Overview

Definitions

Anti-collision loop

An algorithm used to identify and handle a dialogue between a reader and one or more tags in its antenna field.

Hex notation

A hexadecimal value is marked with the suffix ‘h’, i.e. A1h has the value A1 hexadecimal.

ASCII notation

ASCII characters are listed within apostrophes, i.e. ‘x’ means a single x.

Abbreviations

Abbreviation	Description
AID	Application ID
ASCII	American Standard Code for Information Interchange
ATR	Answer to Reset
ATS	Answer to Select
Block	For the Mifare® Standard one block contains 16 bytes
CID	Card Identifier (logical card address, ISO 14443-4)
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard, for more details about DES refer to [3].
EDC	Error Detection Code
EOF	End of Frame
Hex / xxh	Value in Hexadecimal notation
I-block	Information block
LSB	Least Significant Bit or Byte
MSB	Most Significant Bit or Byte
NAD	Node Address (ISO 14443-4)
OSI	Open System Interconnection
OTP	One time programmable
PCB	Protocol Control Byte (ISO 14443-4)
PCON	Protocol Configuration byte of the reader
PPS	Protocol and Parameter Selection
RATS	Request for Answer to Select
R-block	Receive ready block
REQA	Request ISO Type A
REQB	Request ISO Type B
RFU	Reserved for Future Use

© 2008 HID Global Corporation. All rights reserved.

Abbreviation	Description
S-block	Supervisory block
Sector	For the Mifare® Standard one sector contains 4 blocks
SID	Station ID
SFGT	Guard time after RATS
SN	Serial Number of a tag (a 32 bit number)
SOF	Start of frame
TDES	Triple DES
Value block	32 bit data block format. Used in ticketing application
<CR>	Carriage return (0Dh)
<LF>	Line feed (0Ah)

Supported tags

Tag	Manufacturer	Serial number	Read/Write operation	Transfer command	Comments
ISO 14443 A					
MIFARE® Standard	NXP	√	√	√	
MIFARE® 4k	NXP	√	√	√	
MIFARE® Ultralight	NXP	√	√	√	
MIFARE® ProX	NXP	√	√	√	
MIFARE® DESFire	NXP	√	-	√	
MIFARE® Mini	NXP	√	√	√	
SLE66CLX320P	Infineon	√	-	√	encryption not included
SLE 55R04 / 08	Infineon	√	-	√	encryption included
Smart MX	NXP	√	-	√	
Jewel	Innovision	√	√	√	
Topaz	Innovision	√	√	√	
ISO 14443 B					
SLE6666CL160S	Infineon	√	-	√	
SR176	STM	√	√	√	

© 2008 HID Global Corporation. All rights reserved.

Tag	Manufacturer	Serial number	Read/Write operation	Transfer command	Comments
SLIX 4K	STM	√	√	√	
ASK GTML2 ISO	ASK	√	-	√	
ASK GTML	ASK	√	-	√	extended setup needed
Sharp B	Sharp	√	-	√	
TOSMART P0032/64	Toshiba	√	-	√	
Dual Interface					
ISO 14443 A compliant[1]	various	√	-	√	
ISO 14443 B compliant[2]	various	√	-	√	

[1] Performance varies

[2] Performance varies

© 2008 HID Global Corporation. All rights reserved.

1 The MIFARE® Transponder Family

The MIFARE® transponder family consists of various 13.56 MHz transponder ICs, all compliant to the ISO 14443 standard.

1.1 MIFARE® Standard

The MIFARE® Standard card consists of 16 sectors. A sector includes four blocks of 16 bytes each.

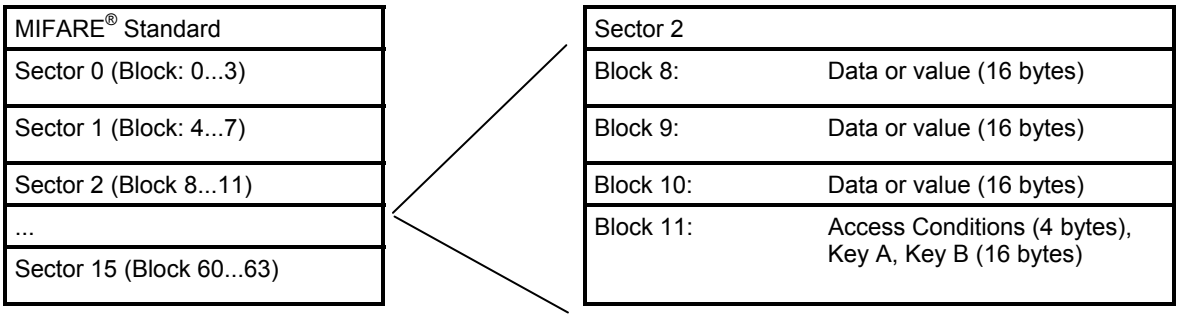

MIFARE® Standard
Sector 0 (Block: 0...3)
Sector 1 (Block: 4...7)
Sector 2 (Block 8...11)
...
Sector 15 (Block 60...63)
Sector 2
Block 8: Data or value (16 bytes)
Block 9: Data or value (16 bytes)
Block 10: Data or value (16 bytes)
Block 11: Access Conditions (4 bytes), Key A, Key B (16 bytes)

Figure 1 MIFARE® Standard: sector diagram

1.1.1 Sector 0 / Block 0

Block 0 is read only.

Serial Number (4 bytes)	Check byte (1 byte)	Manufacturer data (11 bytes)

Figure 2 MIFARE® Standard: sector 0 / block 0

1.1.2 Blocks 3, 7, 11, 15 ...

Transport keys are set on delivery:

Key A (6 bytes)	Access Conditions (4 bytes)	Key B (6 bytes)

Figure 3 MIFARE® Standard: block 3, 7, 11, 15, …

Key A

A0 A1 A2 A3 A4 A5 (Infineon) or FF FF FF FF FF FF (new Philips cards)

Key B

B0 B1 B2 B3 B4 B5 (Infineon) or FF FF FF FF FF FF (new Philips cards)

Access Conditions

FF 07 80 xx (key A is used to read or write; key A itself is not readable; key B is data only). For further information refer to the MIFARE® card manual.

© 2008 HID Global Corporation. All rights reserved.

Remarks

Enabled keys are always read as 00 00 00 00 00 00

Using key B as a data area will cause a security gap, due to the fact that it is necessary to rewrite key A and the access conditions at each write process. It is not recommended to use key B as a data storage area.

All MIFARE® cards use the following state diagram.

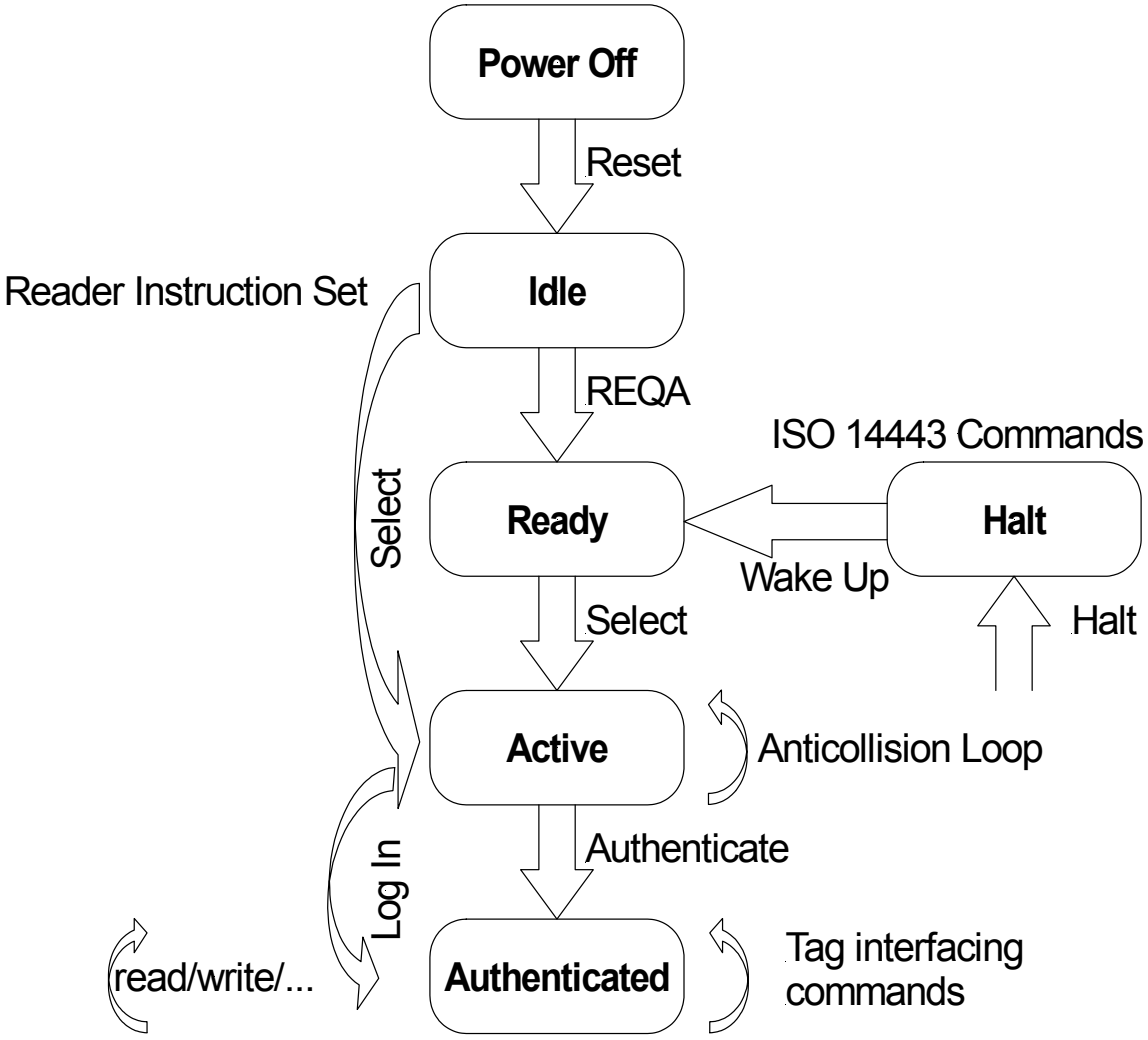


Figure 4 State diagram

© 2008 HID Global Corporation. All rights reserved.

1.2 MIFARE® Ultralight

MIFARE® Ultralight cards have no encryption included. They only support plain text data transmission.

MIFARE® Ultralight only supports 4 bytes per sector, but the command set uses 16 bytes per sector. Only the 4 least significant bytes are valid when using MIFARE® Ultralight.

Ensure that the other bytes match with the tag content when using the write command; otherwise the read back will fail.

1.3 MIFARE® 4k

MIFARE® 4k cards have an increased memory. Beginning from sector 32 (20h), sectors have 16 blocks. Due to compatibility reasons, the sector indices have changed according to the following table. The login sector has to be used to access the corresponding sector on the card.

Table 1 MIFARE® 4k sector index table

Sector	Block	Login sector
00h	00h – 03h	00h
01h	04h – 07h	01h
…	…	…
1Fh	7Ch – 7Fh	1Fh
20h	80h – 8Fh	20h
21h	90h – 9Fh	24h
22h	A0h – AFh	28h
23h	B0h – BFh	2Ch
24h	C0h – CFh	30h
25h	D0h – DFh	34h
26h	E0h – EFh	38h
27h	F0h – FFh	3Ch

1.4 MIFARE® ProX

MIFARE® ProX tags have an operating system onboard. Data organization depends on the operating system installed on the card. These cards can include additional functionalities such as DES or a proprietary encipher algorithm.

Before accessing the operating system, the card must be selected. Customized commands are issued using the transfer command.

© 2008 HID Global Corporation. All rights reserved.

1.5 MIFARE® DESFire

This tag supports additional security algorithms (DES, Triple-DES, and MAC) for security sensitive applications.

Addressed are DESFire tags using a specific command set (see Table 19 DESFire Command Set).

1.5.1 Memory organization

The memory of a DESFire card can be personalized to specific requirements. The card can be seen as data storage device like a hard disk in a PC. The memory is divided into a maximum of 28 different applications (directories) with 16 files each. An application has up to 14 keys. Depending on keys and access conditions a file can be accessed in four different ways. Plain data is never secured. Data is secured using a MAC, single DES or triple DES enciphers.

The following figure describes the memory organization of a DESFire card.

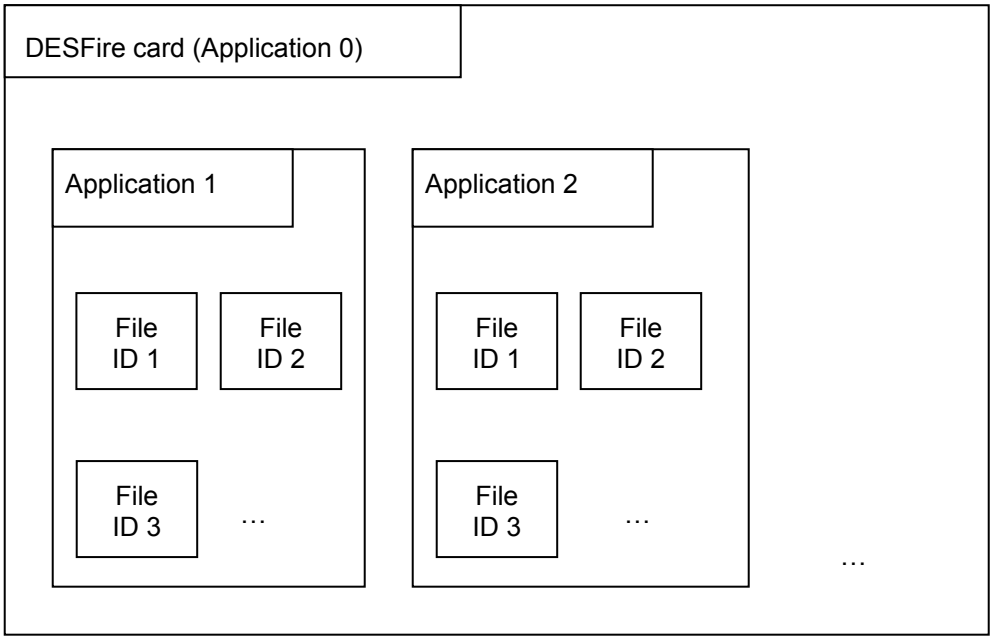


Figure 5 DESFire Memory

© 2008 HID Global Corporation. All rights reserved.

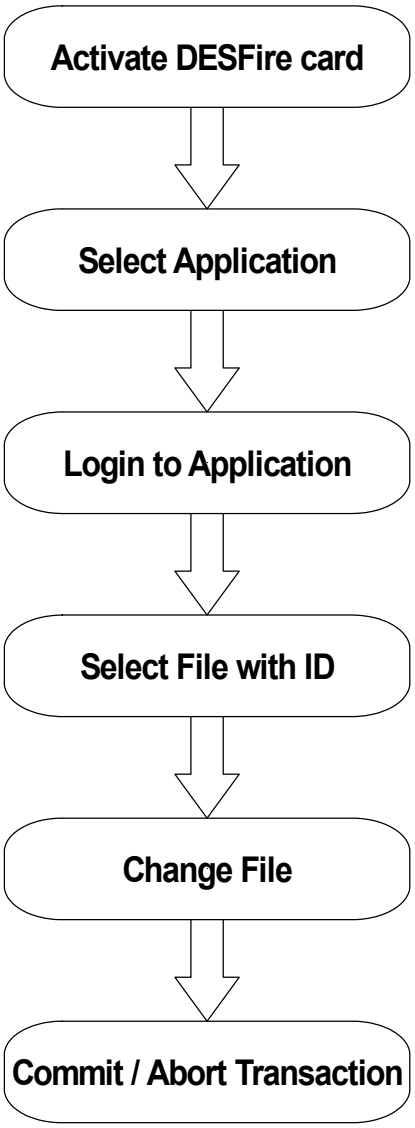


Figure 6 DESFire state diagram

© 2008 HID Global Corporation. All rights reserved.

1.5.1.1 Activate PICC

Before accessing a DESFire card, select the card. A DESFire card has a 7 byte UID. After activation, the card is powered up and ready to accept a DESFire command. Application 0 is selected automatically.

1.5.1.2 Select application

To jump into another application, select the application. An application can be seen as a directory, which contains up to 16 files. The size of the application depends on the stored files.

1.5.1.3 Login to application

Specific access rights can be set for each application. Login to an application allows changing the organization of the application. Login to a file opens a secured file for access. A file can be accessed in four different ways: without any security or secured with MAC, single DES or triple DES.

1.5.1.4 Select file

Before accessing a file, select the file.

1.5.1.5 Change file

Change a selected file according its access rights. If a file is secured, a login is required before changes can be made.

1.5.1.6 Commit / Abort transaction

Value files, backup files, linear record files and cyclic record files only adapt their values after the commit transaction command is given. Several files can be changed within an application at the same time. The abort transactions command annuls all changes within an application. Power loss will cancel all modifications too.

For more details about application settings and access rights refer to [2].

© 2008 HID Global Corporation. All rights reserved.

2 ISO 14443 Type B

ISO 14443 type B cards are supported.

2.1 SR176

The SR176 label contains only 30 bytes of data organized in two bytes per page.

2.1.1 Memory organization

Block address	Byte 1	Byte 0	
0Fh	Lock byte	RFU	Chip ID
0Eh	User data		
…	…		
04h	User data		
03h	Serial number		
02h	Serial number		
01h	Serial number		
00h	Serial number		

2.1.2 Serial number UID

The UID is stored in the first 4 pages. Page 00h contains the LSB of the UID.

Page 03h		Page 02h		Page 01h		Page 00h	
Byte 1h	Byte 0	Byte 1	Byte 0	Byte 1	Byte 0	Byte 1	Byte 0

© 2008 HID Global Corporation. All rights reserved.

2.1.3 Lock byte

The lock byte defines the write access condition of a pair of pages. Each bit can only be set once. This procedure is irreversible. This byte is implemented as an OTP.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Page 0Eh Page 0Fh	Page 0Ch Page 0Dh	Page 0Ah Page 0Bh	Page 08h Page 09h	Page 06h Page 07h	Page 04h Page 05h	Page 02h Page 03h	Page 00h Page 01h

2.1.4 Chip ID

The Chip ID is defined in the low nibble of page 0Fh. It is manufacturer set and is used internally to select and separate single tags.

2.2 SRIX4K

The SRIX4K label contains 512 bytes of data organized into four-byte pages.

2.2.1 Memory organization

Block address	Byte 3	Byte 2	Byte 1	Byte 0
FFh	OTP Lock Reg	ST Reserved	ST Reserved	Fixed Chip ID
7Fh	User data			
…	…			
07h	User data			
06h	32 bits binary counter			
05h	32 bits binary counter			
04h	32 bits Boolean Area			
03h	32 bits Boolean Area			
02h	32 bits Boolean Area			
01h	32 bits Boolean Area			
00h	32 bits Boolean Area			

2.2.2 Lock block

Locking of blocks is not supported with this tag.

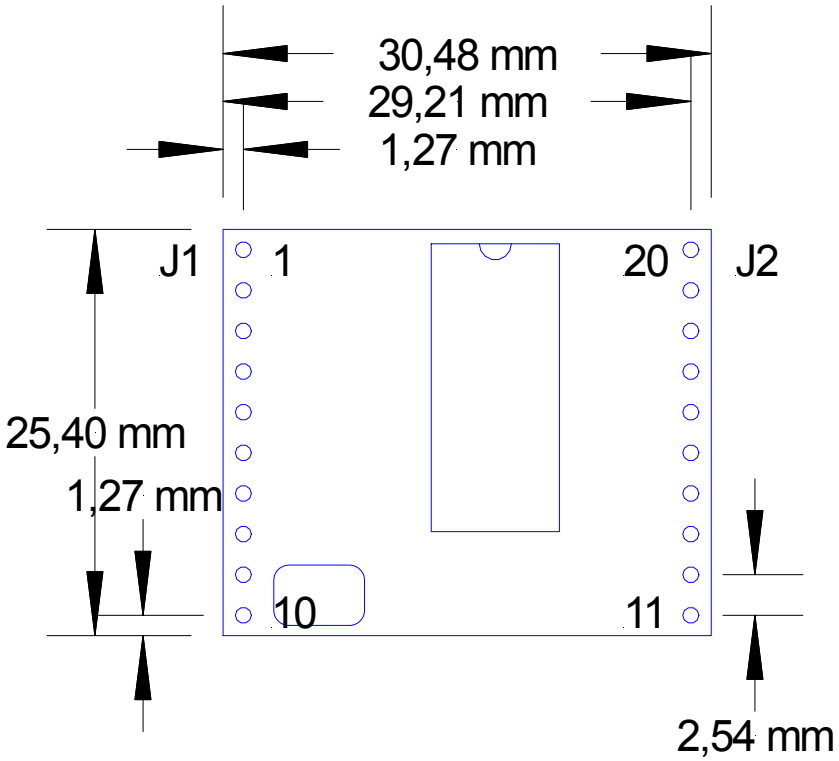
© 2008 HID Global Corporation. All rights reserved.

3 Hardware

© 2008 HID Global Corporation. All rights reserved.

3.1 Pin out of OEM Module RDHO-0401N0-03

Top View



3.1.1 Pin out of J1

PIN	PIN No	Description
ARX	1	Antenna RX
ATX1	2	Antenna TX1
VDD	3	+5 V DC (4.5VDC to 5.5VDC)
GND	4	Ground
ATX2	5	Antenna TX2
TGND	6	Antenna Ground
SAM CLK	7	SAM clock
SAM IO	8	SAM IO
SAM RESET	9	SAM Reset
RFU	10	Reserved for future use

© 2008 HID Global Corporation. All rights reserved.

3.1.2 Pin out of J2

PIN	PIN No	Description
VDD	20	+5 V DC (4.5VDC to 5.5VDC)
GND	19	Ground
LEDg	18	LED green (reading LED)
LEDr	17	LED red
EN	16	Enable reader, open or logic high
MCLR	15	Master clear
USER	14	User Port
DIR	13	Direction of RS 485
TX	12	TX to PC
RX	11	RX from PC

3.1.3 Electrical characteristics of PINs

PIN	PIN No	Voltage	Current (max)	Description
RX TX	11 12	USART[3]	-	To RS232, RS485 or RS422 device driver
USER	14	TTL[4]	25 mA	User sets logic state
MCLR	15	TTL[5]		Master clear Leave unconnected. Low will reset the register and the key management to default values.
EN	16	ST[6]	25 mA	Low will disable the reader device
LEDr	17	TTL	25 mA	Logic Low, used for LED
LEDg	18	TTL	25 mA	With 330 Ω (internal serial) resistor
ARX ATX1 ATX2 TGND	1 2 5 6	(depends on antenna tuning)	200 mA_{PP}	Antenna input Antenna output Antenna output (GND) RF-Output: approx 150mW at 50 Ohms
SAM CLK	7	TTL		Clock for SAM (3.39MHz) With 560 Ω (internal serial) resistor
SAM IO	8	TTL		SAM IO for input and output With a 3.3 kΩ internal pull up resistor and a 330Ω serial resistor

[3] Universal Synchronous Asynchronous Receiver Transmitter

[4] TTL buffer output / input

[5] TTL buffer output / input

[6] Schmitt trigger buffer output

© 2008 HID Global Corporation. All rights reserved.

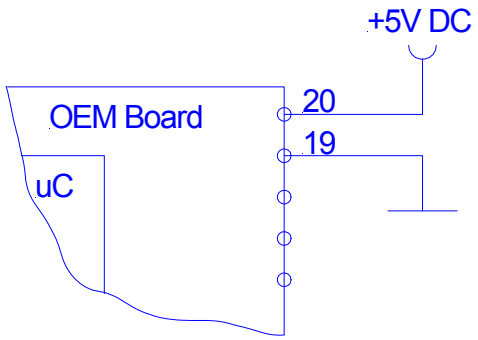
PIN	PIN No	Voltage	Current (max)	Description
SAM RESET	9	TTL		SAM reset
RFU	10	-	-	Not connected
GND	4,19	GND	-	Supply Ground
VDD	3,20	+5 V DC (+4.5V DC to +5.5 VDC)	150 mA	Supply Voltage
DIR	13	TTL	25 mA	RS485 direction

3.1.4 External Connections

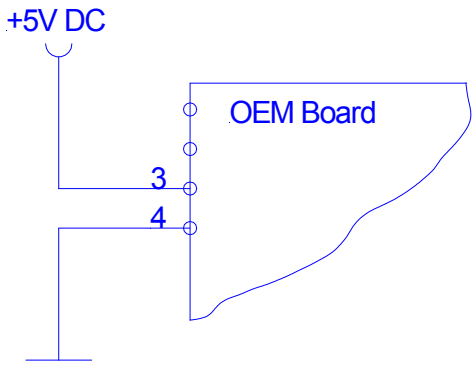
3.1.4.1 Power Supply

If the supply voltage and any noise modulated on the supply voltage remains within the specified limits, no further filtering is required. It is recommended in some cases to use additional filtering for the power supply line. Insufficient power line filtering could cause unexpected or irregular performance drops.

Option 1



Option 2

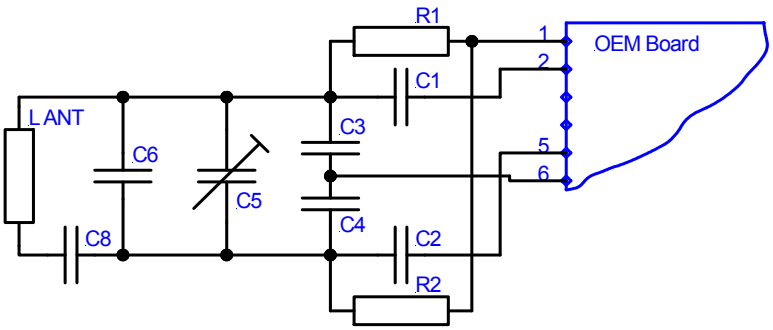


Connect the board as shown above. Both alternatives are possible and can be used as they fit best into the layout of the carrier board. The two VCC PINs and the two GND PINs are connected internally.

© 2008 HID Global Corporation. All rights reserved.

3.1.4.2 Antenna

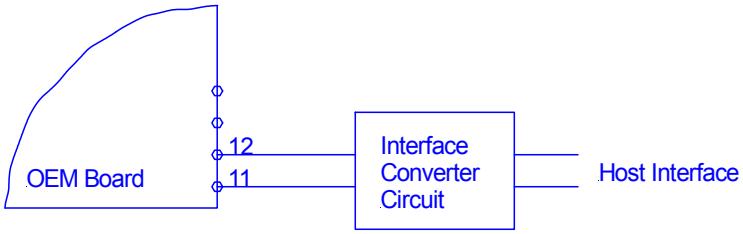
The external antenna needs to have the right inductance and a certain resistor and capacitor combination for optimized frequency tuning and antenna matching.



More Details about the antenna design are available in the Antenna Design Guide. Download his Document from www.hidglobal.com/omnikey.

3.1.4.3 Serial Interface

Connect the OEM Board directly with a micro controller. Alternatively, connect the OEM Board to most serial interface types by using the right interface converter circuit. In order to optimize the communication quality the specific application note of the interface converter circuit needs to be taken into consideration.

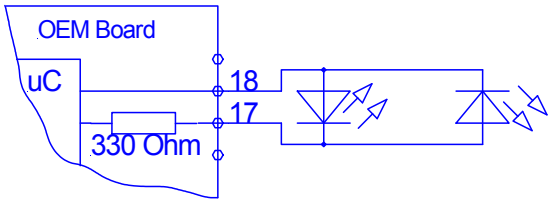


© 2008 HID Global Corporation. All rights reserved.

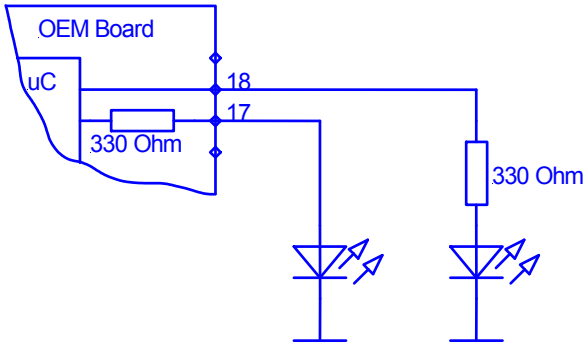
3.1.4.4 Function Control LEDs

Connect two external LEDs to the OEM Board. There are two alternatives possible.

Option 1



Option 2



In both cases, the LED supply voltage levels are TTL levels.

© 2008 HID Global Corporation. All rights reserved.

4 Software

By default, data is transmitted at 9600, n, 8, 1, no handshaking. Two protocol modes are supported. The protocol mode is configured in the reader EEPROM. As factory default, the ASCII protocol is used.

4.1 ASCII Protocol

This protocol is designed for easy handling. The commands are issued using a terminal program. Data is transmitted as ASCII hexadecimal that can be displayed on any terminal program (i.e. HyperTerminal).

Table 2 ASCII protocol frame

Command	Data
Variable length	Variable length

4.2 Binary Protocol

This protocol is designed for industrial applications with synchronization and frame checking. An addressing byte for party line (master/slave, multi-drop) is also included.

The protocol usually requires a device driver. Data is transmitted in binary mode. The reader uses an internal binary watchdog timer to ensure correct framing.

Table 3 Binary Frame Version 1

STX	Station ID	Length	Data	BCC	ETX
1 byte	1 byte	1 byte	Variable length	1 byte	1 byte

The binary frame version 2 is only sent to the host. It is implemented to give extended information to the host.

Enable version 2 in the Protocol configuration 2 register.

Table 4 Binary Frame Version 2

STX	Station ID	Length	Flags	Data	BCC	ETX
1 byte	1 byte	1 byte	1 byte	Variable length	1 byte	1 byte

4.2.1 STX

Start of transmission (02h)

4.2.2 Station ID

Unique ID of the station

00h: Reserved for the bus master. Readers send response to this device ID.

FFh: Broadcast message. All devices will execute the command and send their response.

© 2008 HID Global Corporation. All rights reserved.

4.2.3 Length

Length defines the length of the data block, including the flag byte, if binary protocol version 2 is activated.

If length is set to zero, 256 data bytes are transmitted. The reader module only can send 256 data bytes, but cannot receive commands with 256 bytes.

4.2.4 Flags

The flag byte gives additional information to the host.

Bit 3 – Bit 7	Bit 1 – Bit 2	Bit 0
RFU	Leading Character Info	Error State

Error State

If cleared, the command was processed successfully.

If Error State is set, an error occurred.

Leading Character Info

Bit 1 & 2 defines how to interpret the data in the binary frame.

Bit 2	Bit 1	Description
0	0	No leading character available, all values are hexadecimal.
0	1	The data contains one leading character.
1	0	All data bytes are characters.
1	1	RFU

4.2.5 Data

This part contains the command and the data. The command values are the same as in ASCII protocol mode (‘x’, ‘s’ …) whereas data is transmitted in binary mode.

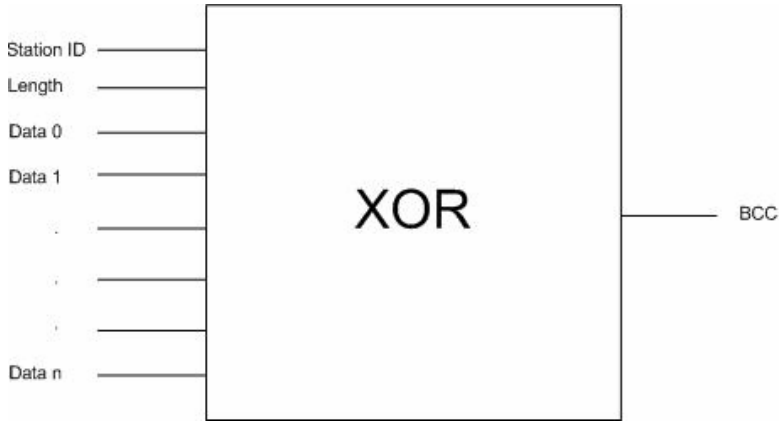
The length of the command block depends on the instruction.

© 2008 HID Global Corporation. All rights reserved.

4.2.6 Block Check Character (BCC)

The BCC is used to detect transmission errors. The BCC is calculated XOR-ing each byte of the transmission frame excluding the STX/BCC and ETX characters. The flags are part of the data.

$$BCC = (StatID)\,XOR\,(Length)\,XOR\,(Command/Data_0)\,XOR\ldots XOR\,(Command/Data_N)$$



4.2.7 ETX

End of transmission. (03h)

4.2.8 Remarks

If the reader device receives an invalid instruction frame (i.e. wrong BCC) or the requested station ID does not match the internal ID of the reader, the command is not executed. The reader waits for the next valid frame.

Use the automatic binary time-out (see Table 5 Protocol configuration register) to detect incomplete binary frames.

4.2.9 Examples

02h	64h	01h	78h	1Dh	03h
STX	Station ID	Length	'x'	BCC	ETX

This instruction frame will reset the reader module with the station ID 64h.

4.3 Register Set

The reader has several system flags used for customization purposes. The flags are stored in its non-volatile EEPROM. The reader accepts changes to these settings only during the start-up phase. Clearing all RFU bits is recommended in order to guarantee compatibility with future releases.

The reader can store up to 32 authentication keys internally to login standard MIFARE® cards. An additional 32 keys can be stored for DESFire authentication. All keys are read only and cannot be accessed via the interface lines.

© 2008 HID Global Corporation. All rights reserved.

4.3.1 EEPROM memory organization

Register	Description
00h … 04h	Unique device ID; read only
05h … 09h	Administrative data; read only
0Ah	Station ID
0Bh	Protocol configuration
0Ch	Baud rate
0Dh	Command Guard Time
0Eh	Operation Mode
0Fh	Single shot time-out value
10h	Internal use / Do not change
11h	Internal use / Do not change
12h	Internal use / Do not change
13h	Protocol configuration 2
14h	Reset Off Time
15h	Reset Recovery Time
16h	Application Family Identifier
17h	ISO 14443A Selection Time-out
18h	ISO 14443B Selection Time-out
19h	SR176 Selection Time-out
1Ah	ISO 15693 Selection Time-out
1Bh	Protocol configuration 3
1Ch	Page Start
1Dh	Internal use / Do not change
1Eh	Internal use / Do not change
1Fh	Page number
20h	Protocol configuration 4
21h	CID
22h	Internal use / Do not change
23h	Internal use / Do not change
24h	Internal use / Do not change
25h	Internal use / Do not change

4.3.2 Unique device ID (00h – 04h)

The unique device ID identifies a reader module. It is factory programmed and cannot be changed.

© 2008 HID Global Corporation. All rights reserved.

4.3.3 Station ID (0Ah)

The station ID is used in binary mode to address a device in party line set up. The station ID can range from 01h to FEh and can be set freely. The value 00h is reserved for the bus master. All readers send their response to this device.

The broadcast message (FFh) forces all readers to response to the command.

Default value is 01h.

4.3.4 Protocol configuration (0Bh)

The protocol configuration register (PCON) specifies general behavior of the reader device.

Default value is 41h.

Table 5 Protocol configuration register

Protocol configuration register							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Extend-ed ID	Extend-ed Protocol	Single-shot	LED	New serial mode	Multitag	Protocol	Auto- start

4.3.4.1 Auto start (default 1)

If set, the reader device will start up in continuous read mode automatically.

4.3.4.2 Protocol (default 0)

If Protocol is set to ‘1’, then the reader uses binary protocol mode. Refer to binary protocol for further information on the binary protocol format.

Default setting = ASCII protocol (0).

4.3.4.3 Multitag (default 0)

The Multitag flag will enable multi-tag recognition in continuous read mode. All tags are detected and displayed. Due to the more complex search algorithm, the continuous read command decreases its detection speed.

4.3.4.4 New Serial Mode (default 0)

If New Serial Mode is set to ‘1’, new serial mode is enabled. A leading character is added to the serial number.

Leading Character	Description
J	ISO 14443 A Jewel tag
M	ISO 14443 A
S	SR 176
Z	ISO 14443 B

4.3.4.5 LED (default 0)

If set the reader suppresses any LED activity. The user manages the state of the LEDs.

© 2008 HID Global Corporation. All rights reserved.

4.3.4.6 Single Shot (default 0)

If Single Shot is set, the reader displays the serial number of a tag in continuous read mode once within a specified time-out. The time-out is defined at EEPROM register 0Fh.

The delay time can be adjusted stepwise in 100ms steps. 00h indicates no delay and FFh indicates infinite delay.

4.3.4.7 Extended Protocol (default 1)

If Extended Protocol is set, the transfer data telegram command supports ISO14443-4 and automatically process the WTX and chaining for smaller frames.

If sending ISO 14443-3 commands this flag has to be switched off.

The transfer data telegram command is only supported in normal mode, not in transmit / receive mode.

4.3.4.8 Extend ID (default 0)

If Extend ID is set, the reader extends the serial number with additional information.

ISO 14443 A tags

Table 6 ISO 14443 A Extended Serial number of part 3 selection

Tag type / ReqA	Serial number	[SAK]
1 byte / 2 bytes	4 / 7 / 10 bytes	1 byte

Table 7 ISO 14443 A Extended Serial number of part 4 selection

Tag type / ReqA	Serial number	[SAK]	ATS	Used Speed	[CID]
1 byte / 2 bytes	4 / 7 / 10 bytes	1 byte	n bytes	1 byte	1 byte

The tag type byte indicates the type of cascade level.

Table 8 ISO 14443 A tag type

Tag type	Description
00h	Cascade level 1 transponder
01h	Cascade level 2 transponder
02h	Cascade level 3 transponder

ISO 14443 B tags

Table 9 ISO 14443 B Extended Serial number of part 3 selection

Serial number	Application data	Protocol info	MBLI/CID
4 bytes	4 bytes	3 bytes	1 byte

Table 10 ISO 14443 B Extended Serial number of part 4 selection

Serial number	Application data	Protocol info	MBLI / CID	Used Speed	[CID]
4 bytes	4 bytes	3 bytes	1 byte	1 byte	1 byte

For detailed description of Application Data, Protocol Info and MBLI/CID, refer to the ISO 14443 documentation [1].

© 2008 HID Global Corporation. All rights reserved.

4.3.5 BAUD, Baud rate control register (0Ch)

The baud rate register defines the communication speed of the reader device.

Default value is 00h.

Table 11 Baud rate register

Baud rate register							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU	RFU	RFU	RFU	RFU	BS2	BS1	BS0

This register defines the baud rate of the device.

Table 12 Baud rate settings

BS2	BS1	BS0	Baud rate
0	0	0	9600 baud (default)
0	0	1	19200 baud
0	1	0	38400 baud
0	1	1	57600 baud
1	0	0	115200 baud
1	0	1	230400 baud (depends on the used interface chip)
1	1	0	460800 baud (depends on the used interface chip)

With the high baud rates (230400 and 460800 baud), proper operation depends on the interface chip used. Please note that some of the interface chips available do not support these high baud rates.

The following table describes the exact baud rates used by the reader.

Table 13 Exact baud rates

Baud rate	Exact baud rate	Difference
9600 baud	9576 baud	-0.25 %
19200 baud	19261 baud	0.32 %
38400 baud	38523 baud	0.32 %
57600 baud	58448 baud	1.47 %
115200 baud	113000 baud	-1.91 %
230400 baud	241545 baud	4.84 %
460800 baud	483091 baud	4.84 %

© 2008 HID Global Corporation. All rights reserved.

The following table describes the communication settings

Table 14 Communication settings

Description
8 data bits
No parity bit
1 stop bit
No flow control

4.3.6 Command Guard Time (0Dh)

The Command Guard Time ensures that commands are not sent too fast consecutively. Following commands are sent after the guard time is elapsed. One time slice is around 37,8us. The longest timeout value is 9,6ms (FFh).

The default value is 20h (1,2ms).

4.3.7 OPMODE, operating mode register (0Eh)

The operation mode register defines which tag types the reader supports. This register enables fast tag recognition because only defined tag types are requested.

Table 15 Operation mode register

Operation mode register							
Bit 7 (MSB)	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0 (LSB)
RFU	RFU	RFU	RFU	RFU	SR176	ISO 14443B	ISO 14443A

Innovision Jewel tag

Innovision Jewel tag is part of ISO 14443 Type A. It can not be separately switched on/off.

4.3.8 Single Shot Time-out (0Fh)

The time-out value defines the delay time between two responses of the reader. It only has effect in continuous read mode. To enable the time-out, the single shot flag has to be set. See the protocol configuration register above. One time-out slice is around 100ms. Exact timing depends on the protocol used.

Value 00h indicates no delay time.

Default value is 0Ah (1 second).

© 2008 HID Global Corporation. All rights reserved.

4.3.9 Protocol configuration 2 (13h)

The protocol configuration register 2 (PCON2) further specifies the general behavior of the reader device.

Default value is 00h.

Protocol configuration 2 register							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Disable ISO 14443 - 4 Error Handling	Enable ISO 14443B Anti-collision	Reset Recovery Time Multiplier		Noisy Environment	Enable binary frame v2	Disable start-up message	Disable multi-tag reset

4.3.9.1 Disable multi-tag reset (default 0)

If set, the reader does not reset before the multi-tag list and multi-select command have been performed.

4.3.9.2 Disable start-up message (default 0)

If Disable start-up message is set, the reader suppresses the start-up message in ASCII mode. This flag is ignored in binary protocol mode.

4.3.9.3 Enable binary frame v2 (default 0)

If Enable binary frame v2 is set, the reader sends version 2 binary frames.

The get station ID command always sends version 1 binary frames!

4.3.9.4 Noisy Environment (default 0)

If Noisy Environment is set, the continuous read mode can only be aborted with the '.' character. When working in a noisy environment, the probability for a reception of an arbitrary/stochastic signal is quite high. This implies a high probability of an unintentional command execution. To reduce this probability, only one character (out of 255) is chosen (‘.’) to be interpreted as the continuous read stop command.

4.3.9.5 Reset Recovery Time Multiplier (default 0)

Multiplies the Reset Recovery Time, including the recovery time of the field reset command.

Reset Recovery Time Multiplier	Reset Recovery Time
0	1x
1	2x
2	3x
3	4x

4.3.9.6 Enable ISO14443 B Anti-collision (default 0)

If set, the anti-collision algorithm for ISO 14443 B tags is enabled.

4.3.9.7 Disable ISO 14443-4 Error Handling (default 0)

If Disable ISO 14443-4 Error Handling is set, ISO14443-4 Error Handling is disabled. The error handling always uses the TMR time-out.

© 2008 HID Global Corporation. All rights reserved.

4.3.10 Reset Off Time (14h)

The Reset Off Time register represents the field off time in ms.

This register is used for the select, continuous read and multi-tag commands.

Default value is 0Ah.

4.3.11 Reset Recovery Time (15h)

The Reset Recovery Time register represents the recovery time in ms after the field is turned on.

This register is used for the select, continuous read and multi-tag commands.

Default value is 25h.

4.3.12 Application Family Identifier (16h)

The AFI (Application Family Identifier) is only supported for ISO14443B and ISO15693 tags. If the set value is different from 00h, the AFI is used. Only transponders with an identical AFI will answer to the reader.

Default value is 00h.

4.3.13 Selection Time-out ISO 14443A (17h)

The Selection Time-out represents the reader card communication time-out for the select, high-speed select, continuous read, multilist, multi-select and MIFARE® login command with ISO 14443A tags. Use low values for a better reaction time between the card and the reader. One time slice is around 300us.

The default value is 10h.

4.3.14 Selection Time-out ISO 14443B (18h)

The Selection Time-out represents the reader card communication time-out for the select, high-speed select, continuous read, multilist and multi-select commands with ISO 14443B tags. For a better reaction time, use low values. One time slice is around 300µs.

The default value is 10h.

4.3.15 Selection Time-out SR176 (19h)

The Selection Time-out represents the reader card communication time-out for the select, continuous read, multilist and multi-select command with SR176 tags. For a better reaction time, use low values. One time slice is around 300µs.

The default value is 10h.

4.3.16 Selection Time-out ISO 15693 (1Ah)

The Selection Time-out represents the reader card communication time-out for the select, high-speed select, continuous read, multilist, multi-select and MIFARE® login command with ISO 15693 tags. Use low values for a better reaction time between the card and the reader. One time slice is around 300us.

The default value is 20h.

© 2008 HID Global Corporation. All rights reserved.

4.3.17 Protocol configuration 3 (1Bh)

The protocol configuration register 3 (PCON3) further specifies the general behavior of the reader device.

Default value is 00h.

Table 16 Protocol configuration register

Protocol configuration 3 register							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
SAK Extended ID	ReqA Extended ID	Internal use / do not change			Page Read	RFU	Disable automatic ISO 14443-4 timeouts

4.3.17.1 Disable automatic ISO 14443-4 timeouts (default 0)

If Disable automatic ISO 14443-4 timeouts is set the automatic ISO 14443-4 timeouts are disabled. The timeouts specified with TMR registers are used.

4.3.17.2 Page read (default 0)

If set the continuous read mode retrieves the content of the tag instead of the serial number. The register Page Start (1Ch) defines the start block and the Page Number (1Fh) defines the number of blocks to be read.

4.3.17.3 ReqA Extended ID (default 0)

If set the Extended ID information for ISO14443 A tags replaces the cascade level information (1 byte) with Request A answer (2 bytes).

4.3.17.4 SAK Extended ID (default 0)

If set the Extended ID information for ISO 14443 A tags will include the SAK byte behind the serial number.

4.3.18 Protocol configuration 4 (20h)

The protocol configuration register (PCON4) specifies general behavior of the reader device.

Default value is 00h.

Table 17 Protocol configuration register

Protocol configuration register							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU	RFU	RFU	RFU	Internal use / do not change	CID Extended ID	WupA/B	Disable Read after Write

4.3.18.1 Disable Read after Write (default 0)

If set, the reader device will not make a read after write for the block write commands "w", "wb", "wd" and "wv".

If the read after write is deactivated, acknowledge from the write commands is a 00h byte instead of the written data.

© 2008 HID Global Corporation. All rights reserved.

4.3.18.2 WupA/B (default 0)

If set, the reader device will use WupA/B instead of ReqA/B during selection of an ISO 14443 tag. Supported commands are select, high-speed select and multi-select.

4.3.18.3 CID Extended ID (default 0)

If set, the extended ID information for ISO 14443 A/B tags will be extended with the CID information only for the high-speed select. The CID byte will be appended on the end of the output.

4.3.19 CID (21h)

The Card Identifier (CID) is used to activate multiple ISO 14443-4 cards at the same time. If only one tag at the same time is used this value should be left 0.

Default value is 00h.

4.3.20 User data (80h - EFh)

These registers are for free use.

4.3.21 Instruction Set

Following table describes all the commands of the reader device. Each command returns an answer to the host. Exceptions are mentioned explicitly. The green LED acknowledges a successfully executed command. The red LED indicates an error.

4.3.22 Common Commands Overview

Table 18 Command overview

Command	Description
'!'	Test continuous read / Check KTT upload status
'c'	Continuous read
'.'	Abort continuous read, refer to continuous read
'dg' / 'dn' / 'dr'	Set LED
'ds'	DES encryption / decryption of data
'g'	Get ID
'h'	High-speed select
'k'	Lock block
'm'	MultiTag select / tag list
'o+a' / 'o+b' / 'o+d' / 'o+e' / 'o+i' / 'o+s' / 'o+v'	Include tag type
'o-a' / 'o-b' / 'o-d' / 'o-e' / 'o-i' / 'o-s' / 'o-v'	Exclude tag type
'oa' / 'ob' / 'od' / 'oe' / 'oi' / 'ot' / 'os' / 'ov'	Set tag type
'of'	Set configuration flags
'og'	Set configuration register
'ox'	Reread all register
'poff' / 'pon'	Antenna power off/on

© 2008 HID Global Corporation. All rights reserved.

Command	Description
'pr' / 'pw'	Read / write user port
'q'	Quiet
'ra'	Resend last answer
'r' / 'rb'	Read block
'rd'	Read data (multiple blocks)
'rp'	Read EEPROM register
's'	Select
'v'	Get version
'w' / 'wb'	Write block
'wd'	Write data (multiple blocks)
'wp'	Write EEPROM register
'x'	Reset
'y'	Field reset
ISO 14443 Type A (MIFARE®) only commands	
'+'	Increment value block (credit)
'-'	Decrement value block (debit)
'='	Copy value block (backup)
'l'	Login (authenticate tag)
'rv'	Read value block
'wv'	Write value block
SR176 only commands	
'k'	Lock block

Table 19 DESFire Command Set

DESFire command set	
0Fh	Create Standard Data File
10h	Create Backup Data File
11h	Create Value File
12h	Create Linear Record File
13h	Create Cyclic Record File
14h	Delete File
15h	Read Data / Records
16h	Write Data / Record
17h	Get Value
18h	Credit
19h	Debit
1Ah	Limited Credit
1Bh	Clear Record File
1Ch	Commit Transaction
1Dh	Abort Transaction
0Fh	Create Standard Data File
10h	Create Backup Data File
11h	Create Value File
12h	Create Linear Record File

© 2008 HID Global Corporation. All rights reserved.

DESFire command set	
13h	Create Cyclic Record File
14h	Delete File
15h	Read Data / Records
16h	Write Data / Record
17h	Get Value
18h	Credit
19h	Debit
1Ah	Limited Credit
1Bh	Clear Record File
1Ch	Commit Transaction
1Dh	Abort Transaction

4.3.23 Error Codes

Following figure shows an overview of all error messages of the reader device.

Table 20 Error codes

Error Code	Description
'?'	Unknown command
'C'	Collision or CRC/MAC Error
'F'	General failure
'I'	Invalid value format, specified block does not match the value format
'N'	No tag in the field
'O'	Operation mode failure or file not selected
'R'	Command parameter out of range
'X'	Authentication failed
Xxh	DESFire error code

© 2008 HID Global Corporation. All rights reserved.

4.3.24 Common commands

4.3.24.1 Test Continuous Read

This command tests the state of the continuous read command.

This command only works in ASCII mode.

Command

Command	Data
'!'	None

Answer

Answer	Description
'F'	Continuous read mode is not active.
'!'	Continuous read mode is active.

4.3.24.2 Continuous Read

The reader device reads and displays serial numbers continuously while one or more tags remain in the field. This command stops if any character is sent to the reader module. The reader module returns the character ‘S’ (53h).

The reader supports different tag types at the same time. To increase the reading performance switch to a single tag mode. If more than one tag of the same type should be detected at the same time, the Multitag flag must be activated. The response data length depends on the tag type.

Command

Command	Data
'c'	None

Answer

Answer	Description
Data	Serial number (n bytes)
'N'	Error: No Tag in the field (only binary protocol)

4.3.24.2.1 Multitag continuous read mode

If the Multitag flag is set in the Protocol Configuration (PCON) register the reader reads multiple tags continuously.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.2.2 Auto start

The continuous read mode is started automatically in ASCII mode. The auto start flag must be set in the PCON register.

4.3.24.2.3 Noisy Environment

If the Noisy Environment flag is set, the continuous read mode can only be aborted with the '.' character.

4.3.24.2.4 Binary mode

This command is not fully supported in binary protocol mode.

Continuous Read in binary mode does not start-up automatically at boot time, even if the corresponding EEPROM flag is set.

Within the single shot time-out, only one response is sent.

4.3.24.2.5 Simple access control applications

Serial numbers are always sent plain. Data encryption is activated after a successful login.

For simple access control applications the use read-only blocks for the identification of the tag is recommended.

Reading any block (even the manufacturer block) of the transponder will increase your security.

4.3.24.2.6 LED activity

The LED stays green as long as a tag was found and goes dark if the tag is removed from the field.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.3 Set LED

This command controls the LED activity. If the LED flag is set, the automatic LED function is switched off. The user can set the state of the LED manually.

Command

Command	Data
'dg'	None
'dr'	None
'dn'	None

Answer

Answer	Description
'DG' 'DR' 'DN'	String of LED state

Example

Command	Answer	Description
'dg'	DG	Switch on LED green, LED red off
'dr'	DR	Switch on LED red, LED green off
'dn'	DN	Switch off both LEDs

© 2008 HID Global Corporation. All rights reserved.

4.3.24.4 DES encryption / decryption of data

This command returns 8 bytes of encrypted / decrypted data.

Command

Command	Data
'ds'	Options (1 byte) Key (8/16 bytes) / Key Number (1 byte) Data (8 byte)

Answer

Answer	Description
Data	Encrypted / Decrypted data (8 bytes)

Option byte

Option byte							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU	RFU	RFU	RFU	RFU	Encode	Key Length	Key Index

Key Index

If the Key Index is set, the command only needs the key number (1 byte) instead of the key (8/16 bytes).

The key number corresponds to the key number used in the key management.

Key Length

If the Key Length is set, the command uses the TDES algorithm with 16-byte key.

If cleared, the command uses the DES algorithm with 8-byte key.

Encode

Setting this flag encodes the data.

Clearing this flag decodes the data.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.5 Get ID

This command returns the station ID of the reader device. The answer is time slotted to enable the detection of all devices in party line mode.

The station ID has only effect in binary mode.

Command

Command	Data
'g'	None

Answer

Answer	Description
Data	Station ID of the reader device (1 byte)

© 2008 HID Global Corporation. All rights reserved.

4.3.24.5.1 Time slotted answer

In party line mode, more than one reader can be used simultaneously. The time slotted answer allows separating in time the answers from all connected devices. The station ID is used to determine the correct time slot.

The reader supports up to 254 unique time slots. The following formula calculates the duration of one time slot (only one baud rate is supported per party line):

$$T_0[s] = \frac{10}{Baudrate} * 6$$

Figure 7 Time slot formula

The following figure shows the timing diagram of time slotted answers.

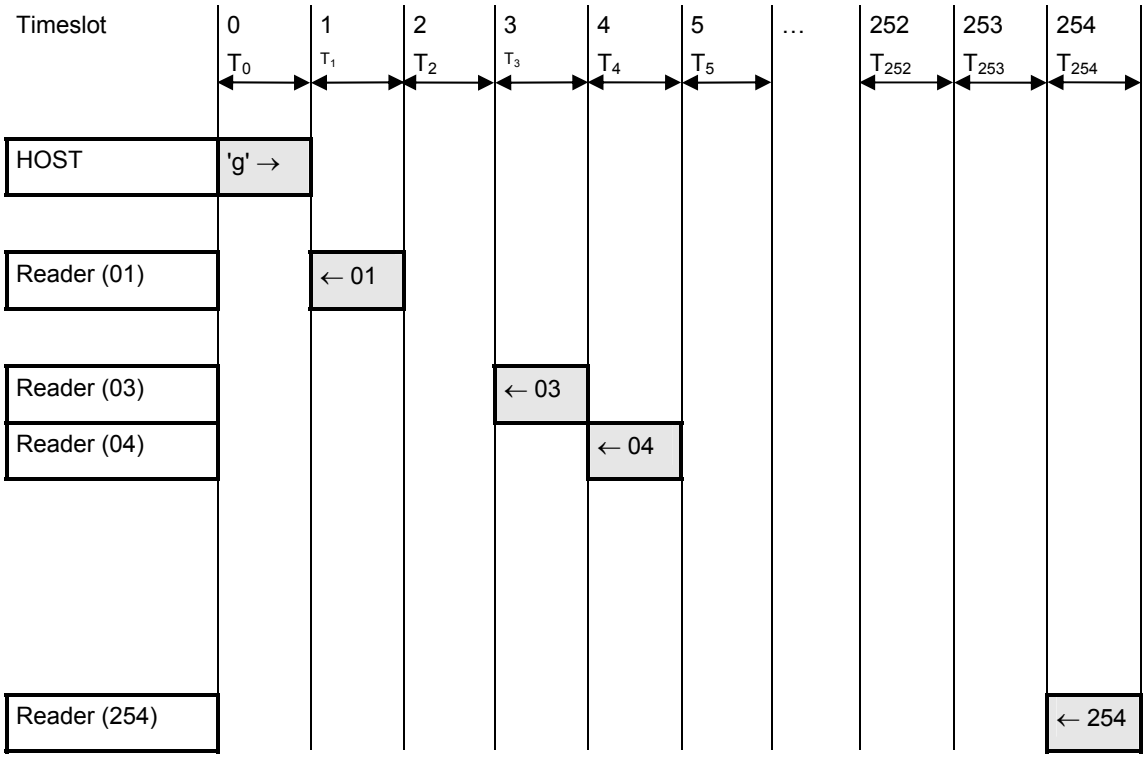


Figure 8 Time slotted answers diagram

© 2008 HID Global Corporation. All rights reserved.

4.3.24.5.2 Binary Protocol Version 2

This command never sends version 2 binary frames.

4.3.24.6 High-speed select

This command selects a card in the antenna field (according to the selection criteria) or prepares a multi-select command, switches to high baud rates and enables 256-byte frames. If execution is successful, the command returns the UID of the selected card and the used baud rate. The reader automatically detects the maximum frame size of the card. The reader also tries to communicate to the transponder with the specified baud rate. If no communication is possible, the reader will automatically decrease the speed to the next lower value.

In synchronous mode the up and downlink speed are identical.
In asynchronous mode the up and downlink speed can be different.

This command can also force the reader to the communication speed and frame size of the tag to the specified values. This is only needed if the high-speed select is done manually with the transfer command.

Command

Command	Data
'h'	Option byte (1 byte) synchronous mode 00h … select a single card with 106kBaud 02h … select a single card with 212kBaud 04h … select a single card with 424kBaud 08h … select a single card with 848kBaud 10h … prepare next multi-select for 106kbaud 12h … prepare next multi-select for 212kbaud 14h … prepare next multi-select for 424kbaud 18h … prepare next multi-select for 848kbaud 20h … forces reader to 106kBaud 22h … forces reader to 212kBaud 24h … forces reader to 424kBaud 28h … forces reader to 848kBaud tag size 30h – 38h … force tag frame size asynchronous mode 80h … select a single card with 106kBaud 82h … select a single card with 212kBaud 84h … select a single card with 424kBaud 88h … select a single card with 848kBaud 90h … prepare next multi-select for 106kbaud 92h … prepare next multi-select for 212kbaud 94h … prepare next multi-select for 424kbaud 98h … prepare next multi-select for 848kbaud

© 2008 HID Global Corporation. All rights reserved.

Command	Data
	A0h … forces reader to 106kBaud from tag to reader A2h … forces reader to 212kBaud from tag to reader A4h … forces reader to 424kBaud from tag to reader A8h … forces reader to 848kBaud from tag to reader B0h … forces reader to 106kBaud from reader to tag B2h … forces reader to 212kBaud from reader to tag B4h … forces reader to 424kBaud from reader to tag B8h … forces reader to 848kBaud from reader to tag

Answer

Answer	Description
Data (n bytes) + frame size and baud rate (1byte)	Serial number + frame size used and baud rate
'F'	Error: General failure
'N'	Error: No Tag in the field

Note: If the tag does not support ISO 14443 part 4 F0h will return after serial number instead of used frame size/baud rate.

Examples

High-speed select

Command	Description
h08	1234567890ABCD84 Select the card with UID 1234567890SABCD. The card supports a 256-byte frame size and 424kBaud on the air interface.

High-speed multi-select

Command	Description
h18 m1234567890ABCD<CR>	Prepare next multi-select for 848kBd 1234567890ABCD84 Select the card with UID 1234567890SABCD. The card supports a 256-byte frame size and 424kBaud on the air interface.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.6.1 Answer from 0xh and 1xh

The lower nibble contains the baud rate used for the air interface.

Table 21 Baud Rate Values

Baud Rate	Description
x0	106kBaud
x2	212kBaud
x4	424kBaud
x8	848kBaud

The higher nibble contains the frame size used for the air interface.

Table 22 Frame Size

Frame Size	Description
0x	16 Bytes
1x	24 Bytes
2x	32 Bytes
3x	40 Bytes
4x	48 Bytes
5x	64 Bytes
6x	96 Bytes
7x	128 Bytes
8x	256 Bytes

© 2008 HID Global Corporation. All rights reserved.

4.3.24.6.2 Answer from 8xh

The lower nibble contains the baud rate used for the air interface.

The value for the baud rate is XORed with the used up and downlink speed.

Table 23 Baud Rate values

Baud Rate	Description
x1	106kBaud
x2	212kBaud
x4	424kBaud
x8	848kBaud

The higher nibble contains the frame size used for the air interface.

Table 24 Frame Size

Frame Size	Description
0x	16 Bytes
1x	24 Bytes
2x	32 Bytes
3x	40 Bytes
4x	48 Bytes
5x	64 Bytes
6x	96 Bytes
7x	128 Bytes
8x	256 Bytes

4.3.24.6.3 Answer from 2xh, 3xh, 9xh, Axh and Bxh

Returned is the option byte as the answer.

4.3.24.6.4 Select a single tag

No previous continuous read is required. The command executes an automatic field reset.

4.3.24.6.5 Extended ID

See above for more information on Extended ID.

The RATS answer is inserted between the serial number and baud rate / frame size byte for ISO14443 A tags.

4.3.24.6.6 Multiple tags

This command with parameter 1xh prepares the next multi-select command as a high-speed select. Any other command will disable the preparation.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.6.7 RATS Guard Time SFGT

A high-speed select with parameters 0xh and 1xh automatically waits the SFGT guard time received from the tag before sending the PPS command.

4.3.24.7 Multi-Tag Selection / List

This command detects several tags at the same time. It replaces the fast select command ('s') in multiple tag surroundings. The Multi-Tag List command lists all tags with their serial numbers. Use the Multi-Tag Select command to select a single tag. Each tag has to be selected separately.

Command

Command	Data
'm'	Serial number (n bytes) <CR> (1 byte)

Answer

Answer	Description
Data	serial number
'N'	Error: No Tag in the field

Example

Command	Description
m<CR>	04E9E700000000 → first card 34030F07 → second card 02 → number of detected tags
m04E9E700000000<CR>	Select card with its serial number

4.3.24.7.1 Multi-tag list

Sending a <CR> as the first parameter, the reader returns a list of all tags present in the antenna field. In the end the total number of tags detected is returned.

4.3.24.7.2 Reading distance

Each card needs a specific amount of power. The reader always provides the same power level. Therefore, the reading distance will decrease if more tags are present. Basically, the reading distance depends on the tag, the antenna and the tuning of the antenna.

4.3.24.7.3 Multi-tag select

Using the serial number with <CR> as parameter, the corresponding tag will be selected. High-level interactions can be performed addressing only this card. All other tags remain silent.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.7.4 Multi-tag reset

The antenna field reset can be deactivated with the Protocol configuration 2 register.

By suppressing the antenna field reset, it is possible to detect only new tags in the antenna field.

4.3.24.7.5 Maximum number of tags

The maximum number of tags in the antenna field is limited to 64 and by the physical characteristics of the antenna.

4.3.24.7.6 LED activity

The LED stays green as long as a tag was found and goes dark if the command is finished.

4.3.24.8 Include tag type

This command includes a specific tag type to those addressed by the reader device.

Command

Command	Data
‘o+’	Tag type (1 byte)

Answer

Answer	Description
'O+' + tag type (1 byte)	Command code + String of tag type

Tag type character

Refer to Set tag type.

Example

Command	Description
o+a	Include ISO14443-A to the tag types addressed by the reader device.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.9 Exclude tag type

This command excludes a specific tag type from being addressed by the reader device.

Command

Command	Data
‘o-’	Tag type (1 byte)

Answer

Answer	Description
'O-' + tag type (1 byte)	Command code + String of tag type

Tag type character

Refer to Set tag type.

Example

Command	Description
o-a	Exclude ISO14443-A from the tag types addressed by the reader device.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.10 Set tag type

This command sets up the reader for a specific tag type. The continuous read function will speed up because only this type of tag is addressed. After a reset, the reader starts as defined in its start-up configuration.

Command

Command	Data
'o'	ISO type (1 byte) 'a' … ISO 14443 Type A 'b' … ISO 14443 Type B 's' … SR176 't' … activate all tags

Answer

Answer	Description
'OA' 'OB' 'OS' 'OT'	String of tag type

Example

Command	Description
oa	Sets the reader device to address ISO14443-A type tags.

Innovision Jewel tag

Innovision Jewel tag is part of ISO 14443 Type A. It can not be separately switched on/off.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.11 Set Configuration Flags

This command allows setting some configuration flags just in time; no reset is needed. The values are not stored in the EEPROM; therefore, the changed values are not available after a reset.

Command

Command	Data
of	flag type (1 byte) data (1 byte)

Answer

Answer	Description
Data (1 byte)	Current state of changed flag.
'R'	Error: Out of range

Example

Command	Description
of0101	Answer: 01 Enables the New Serial Mode flag.

© 2008 HID Global Corporation. All rights reserved.

Flag Types

The following table shows the Flag Type with its corresponding flag from the specified Protocol Configuration Register.

Table 25 Flag Type with corresponding flag

Flag Type	Corresponding Flag	Protocol Configuration Register	Valid values
00h	Multitag	1	00 / 01
01h	New Serial Mode	1	00 / 01
02h	LED	1	00 / 01
03h	Single Shot	1	00 / 01
04h	Extended Protocol	1	00 / 01
05h	Extended ID	1	00 / 01
06h	Disable Multitag Reset	2	00 / 01
07h	Noisy Environment	2	00 / 01
08h	Reset Recovery Time Multiplier	2	00 … 03
09h	Enable ISO14443 B Anti-collision	2	00 / 01
0Ah	Disable ISO14443-4 Error Handling	2	00 / 01
0Bh	Disable automatic ISO14443-4 timeouts	3	00 / 01
0Dh	Page Read	3	00 / 01
11h	ReqA Extended ID	3	00 / 01
12h	Disable Read after Write	4	00 / 01
13h	SAK Extended ID	3	00 / 01
14h	WupA/B	4	00 / 01
15h	CID Extended ID	4	00 / 01
16h	Internal use / Do not change		

4.3.24.11.1 Out of range failure 'R'

The entered flag type is out of range.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.12 Set Configuration Register

This command allows setting some configuration registers just in time; no reset is needed. The values are not stored in the EEPROM; therefore, the changed values are not available after a reset.

Command

Command	Data
og	Register type (1 byte) data (1 byte)

Answer

Answer	Description
Data (1 byte)	Current state of changed register.
'R'	Error: Out of range

Example

Command	Description
og0450	Answer: 50 Sets the Reset Recovery Time to 50h.

Register Types

The following table shows the Register Type with its corresponding register.

Table 26 Register Type with corresponding register

Register Type	Corresponding Register
00h	Single shot time-out value
01h	Internal use / Do not change
02h	Internal use / Do not change
03h	Reset Off Time
04h	Reset Recovery Time
05h	ISO 14443A Selection Time-out
06h	ISO 14443B Selection Time-out
07h	SR176 Selection Time-out
08h	AFI
0Ch	Page Read Start
0Dh	Page Read Number
0Eh	Command Guard Time
0Fh	CID
10h	Internal use / Do not change

© 2008 HID Global Corporation. All rights reserved.

4.3.24.12.1 Out of range failure 'R'

The entered register type is out of range.

4.3.24.13 Reread all register

This command rereads and applies all register settings.

Command

Command	Data
ox	none

Answer

Answer	Description
Data (3 bytes)	'X' + new protocol + new baud rate

Example

Command	Description
ox	Answer: X0106 binary protocol and 460800 baud active

New protocol

00h means ASCII and 01h means binary protocol.

New baud rate

Values of 00h-06h are valid. For baud rate values refer to baud rate register.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.14 Antenna power on/off

This command controls the antenna power. It can be used to decrease the power consumption of the reader.

Command

Command	Data
'pon'	Switch reader on
'poff'	Put reader in standby mode

Answer

Answer	Description
'P'	Positive acknowledge

Example

Command	Description
poff	Put reader in standby mode

4.3.24.14.1 Power off

The reader enters standby mode. Power consumption is decreased. All tags in the antenna field are powered off and reset. Standby mode is only entered manually.

To switch off the whole unit, pin 16 (Enable) has to be set to logic low.

4.3.24.14.2 Power on

The reader leaves standby mode and is ready for the next command. Sending a tag command (i.e. select, continuous read) the reader is powered up.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.15 Read/Write user port

This command sets or reads the state of the user port (pin 14) of the OEM reader device. The port is set either as output or as input.

Command

Command	Data
'pr'	None
'pw'	State of user port (1 Byte)

Answer

Answer	Description
Data	State of user port (1 Byte)
'C'	Error: Error correction fails
'F'	Error: Transmission Error / No answer received

Example

Command	Description
pr	Reads user port
pw01	Sets user port state to high

© 2008 HID Global Corporation. All rights reserved.

4.3.24.15.1 Read port

The port read command returns the current state of the USER port.

Table 27 Read USER port return values

Port state	Description
00h	USER port is low
01h	USER port is high

4.3.24.15.2 Write port

If user port is used as an output, a 1kΩ resistor has to be integrated into the wire. Otherwise, the reader device can be damaged.

Table 28 Write User port settings

Port state	Description
00h	Sets USER port to low
01h	Sets USER port to high
02h – 7Fh	RFU
80h - FFh	Sends a serial data frame and checks the received frame

Sending a Data Frame

If the highest bit (MSB) is set in the State of the User Port, the command sends a serial data frame out the USER port.

The frame includes a start bit, 8 data bits, parity bit and a stop bit.

Table 29 Sending Serial Data Frame

Transmit Frame	Description
Low	Start bit
Low	RFU
Data Bit 6	State of the User Port Bit 6
Data Bit 5	State of the User Port Bit 5
Data Bit 4	State of the User Port Bit 4
Data Bit 3	State of the User Port Bit 3
Data Bit 2	State of the User Port Bit 2
Data Bit 1	State of the User Port Bit 1
Data Bit 0	State of the User Port Bit 0
Parity Bit	Even Parity Bit
High	Stop Bit

© 2008 HID Global Corporation. All rights reserved.

After 2ms Guard Time the answer should be received on the User Port otherwise an error is returned.

Table 30 Receiving Serial Data Frame

Receive Frame	Description
Low	Start bit
Error Bit	If set, an error was detected.
Data Bit 6	State of the User Port Bit 6
Data Bit 5	State of the User Port Bit 5
Data Bit 4	State of the User Port Bit 4
Data Bit 3	State of the User Port Bit 3
Data Bit 2	State of the User Port Bit 2
Data Bit 1	State of the User Port Bit 1
Data Bit 0	State of the User Port Bit 0
Parity Bit	Even Parity Bit
High	Stop Bit

If the Error bit is set or the Parity Bit is not correct, the Write User Port command returns an error code.

4.3.24.16 Quiet

This command sets a selected tag into halt state. Only ISO14443 A+B and SR176 tags are supported.

Command

Command	Data
'q'	None

Answer

Answer	Description
'Q'	Halt state successfully set.
'N'	Error: No Tag in the field

4.3.24.16.1 ISO 14443 Type A

With ISO14443-3 Type A tags, the Quiet command always answers with 'Q' because the halt command does not send any acknowledge.

In Part 4 a 'Deselect' command will be performed.

4.3.24.16.2 ISO 14443 Type B

Some ISO14443 Type B tags do not support this command or do not respond. ‘Quiet’ is an ISO 14443-4 command, so it will work only if the ‘Deselect’ command is supported by the corresponding transponder.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.16.3 SR176

With SR176 tags the Quiet command always answer with 'Q' because the completion command does not send any acknowledge.

4.3.24.17 Resend Last Answer

This command resends the last answer from the internal serial buffer of the reader.

Command

Command	Data
'ra'	Resend last answer

4.3.24.18 Read block

This command reads a data block on a card. The size of the returned data depends on the tag used. The block address range depends on the tag as well.

Command

Command	Data
'r'	Block address (1 byte), valid range 00h – 40h
'rb'	Block address (1 byte)

Answer

Answer	Description
Data	data block (depends on tag type)
'F'	Error: read failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure
'R'	Error: Out of range

Example

Command	Description
rb05	Reads block 05.

4.3.24.18.1 Read failure 'F'

This error is returned if either the reader receives bad data or the block address exceeds the block address range of the sector.

4.3.24.18.2 No tag in field 'N'

The tag does not respond. There is either no tag present or addressed.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.18.3 Operation mode failure 'O'

The presented tag is not ISO14443 type A compliant.

4.3.24.18.4 Out of range failure 'R'

The block address of the 'r' command is higher than 40h.

The block address of the 'r' command conflicts with other commands, therefore the block address has to be limited to 40h.

Use the 'rb' command instead.

4.3.24.19 Read data (multiple blocks)

This command reads multiple data blocks on a card. The size of the returned data depends on the tag used. The block address range depends on the tag as well.

Command

Command	Data
'rd'	Start block address (1 byte) Number of blocks to read (1 byte)

Answer

Answer	Description
Data	data block (depends on tag type)
'F'	Error: read failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
rd0504	Reads 4 blocks starting with block 05.

4.3.24.19.1 Read failure 'F'

This error is returned if either the reader receives bad data or the block address exceeds the block address range of the sector.

4.3.24.19.2 No tag in field 'N'

The tag does not respond. There is either no tag present or addressed.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.19.3 Operation mode failure 'O'

The presented tag is not ISO14443 type A, SR 176 compliant.

For ISO 14443 type A only MIFARE® tags are supported.

4.3.24.20 Read reader EEPROM

This command reads the internal reader EEPROM. It contains all start-up parameters and the device ID. Changes in the start-up settings will only go into effect after a reset of the device.

Command

Command	Data
'rp'	EEPROM address (1 byte) 00h … EFh

Answer

Answer	Description
Data	EEPROM data (1 byte)
'R'	Error: Out of range failure

Example

Command	Description
rp0B	Reads protocol configuration register.

4.3.24.20.1 Out of range failure 'R'

The entered EEPROM address is not valid.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.21 Select

This command selects a single card in the antenna field. It can only be used in single tag mode. If successfully executed, the command returns the UID of the selected card. The reader detects the length of the UID automatically.

Command

Command	Data
's'	None

Answer

Answer	Description
Data	serial number
'N'	Error: No Tag in the field

Example

Command	Description
s	1234567890ABCD Select the card with UID 1234567890SABCD.

4.3.24.21.1 Select a single tag

No previous continuous read is required. The command executes an automatic field reset.

4.3.24.21.2 Extended ID

See above for more information on Extended ID.

4.3.24.21.3 Multiple tags

This command is designed for fast access of a single tag in the field. If multiple cards are used the 'm' instruction has to be used instead.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.22 Get Version

This command returns the current version of the reader module.

Command

Command	Data
'v'	None

Answer

Answer	Description
'Dual 2.2' + <CR> + <LF>	ASCII Mode
02 00 08 44 75 61 6C 20 32 2E 32 32 03	Binary Mode

Example

Command	Description
v	'Dual 2.2' Version of the reader module

4.3.24.23 Write DESFire key

This command is used to store a key into the DESFire key memory of the reader. The reader can store up to 32 keys. DESFire keys can be used for fast access to applications on a card.

Command

Command	Data
'wf'	Key number (1 byte) 00h … 1Fh Key (16 bytes)

Answer

Answer	Description
data	Written key (16 bytes)
'F'	Error: Write failure
'R'	Error: Out of range

Example

Command	Description
wf00001122334455667788 99AABBCCDDEEFF	Store key 00112233445566778899AABBCCDDEEFFh in EEPROM (key number 0).

© 2008 HID Global Corporation. All rights reserved.

4.3.24.23.1 Out of range failure 'R'

The entered key number exceeds the permitted range.

4.3.24.23.2 Writing DESFire Keys

Keys are write only. It is not possible to read the keys. Nevertheless the reader returns correct error messages if the writing process fails.

A verification of the DESFire key can only be done using an appropriate card and following successful login.

4.3.24.23.3 Using DESFire keys for authentication

DESFire keys may be used for DESFire tag authentication or DES/TDES encryption/decryption.

Each key is 16 bytes long and stored redundantly for data security.

4.3.24.24 Write master key

This command stores a MIFARE Standard key into the master key memory of the reader. The reader can store up to 32 keys.

Command

Command	Data
'wm'	Key number (1 byte) 00h … 1Fh Key (6 bytes)

Answer

Answer	Description
data	Written key (6 bytes)
'F'	Error: Write failure
'R'	Error: Out of range

Example

Command	Description
wm00112233445566	Store key 112233445566h in EEPROM (key number 0).
wm02A0A1A2A3A4A5	Store transport key 1 in EEPROM key 2.

4.3.24.24.1 Out of range failure 'R'

The entered key index exceeds the address range.

4.3.24.24.2 Writing master keys

Keys are Write-Only. It is not possible to read the keys. Nevertheless, the reader returns correct error messages if the writing process fails.

A verification of the master key can only be done using an appropriate card and following successful login.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.24.3 Using master keys for authentication

Master keys may be used for ISO-14443 A tag authentication. It is possible to use every stored key for key A as well as key B authentication.

Each key is 6 bytes long and stored redundantly for data security.

4.3.24.25 Write block

This command writes data to a block. A read is done automatically after every write to ensure correct writing.

Command

Command	Data
'w'	Block address (1 byte), valid range 00h – 40h Data (n bytes)
'wb'	Block address (1 byte) Data (n bytes)

Answer

Answer	Description
Data	Data block (depends on tag type)
'F'	Error: Write failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure
'R'	Error: Out of range

Example

Command	Description
wb0511223344	Writes data 11223344 on block 05.

4.3.24.25.1 Write failure 'F'

This error is displayed if bad transmission conditions are given. If the block address exceeds the physical number of blocks of a tag, this error is shown.

4.3.24.25.2 No tag error 'N'

This error is returned if no tag is present or the card does not respond.

4.3.24.25.3 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.25.4 Out of range failure 'R'

The block address of the 'w' command is higher than 40h.

The block address of the 'w' command conflicts with other commands, therefore the block address has to be limited to 40h.

Use the 'wb' command instead.

4.3.24.26 Write data (multiple blocks)

This command writes multiple blocks to a card.

Command

Command	Data
'wd'	Start block address (1 byte) Number of blocks (1 byte) Data (n bytes)

Answer

Answer	Description
Data	Data block (depends on tag type)
'F'	Error: Write failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
wd050211223344556 67788	Writes data 11223344 on block 05 and 55667788 on block 06.

4.3.24.26.1 Write failure 'F'

This error is displayed if bad transmission conditions are given. If the block address exceeds the physical number of blocks of a tag, this error is shown.

4.3.24.26.2 No tag error 'N'

This error is returned if no tag is present or the card does not respond.

4.3.24.26.3 Operation mode failure 'O'

The presented tag is not ISO14443 type A, SR 176 compliant.

For ISO 14443 type A only MIFARE® tags are supported.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.26.4 Disable Read after Write

A read is done automatically after every write to ensure correct writing.

If the "disable Read after Write flag" is set no read is done, and the returned data is a 00h byte in case of successfully written data.

4.3.24.27 Write EEPROM

Writes to the internal reader EEPROM. It contains all start-up parameters and the device ID. Changes to the start-up settings will only go into effect after a reset of the device.

Command

Command	Data
'wp'	Address (1 byte), valid range 0Ah - EFh Data (1 byte)

Answer

Answer	Description
Data	EEPROM data (1 byte)
'F'	Error: Read after write failure
'R'	Error: Out of range failure

Example

Command	Description
wp0A01	Set EEPROM address 0A (Station ID) to 01h

4.3.24.27.1 Out of range failure 'R'

The entered address exceeds the address range.

© 2008 HID Global Corporation. All rights reserved.

4.3.24.28 Reset

This command executes a power on (software) reset. New configuration settings will be loaded. It resets all tags in the antenna field.

Command

Command	Data
'x'	None

Answer

Answer	Description
'Dual 2.2' + <CR> + <LF>	ASCII Mode
None	Binary Mode

4.3.24.28.1 Disable Start-up Message

If the start-up message is disabled in the protocol configuration register 2, the ASCII mode does not respond with the version of the reader.

4.3.24.28.2 Reset Timing

The power up timing depends on environmental conditions such as voltage ramp up. For handheld devices the timing can vary based on the charge state of the battery.

4.3.24.28.3 Field Reset

The field reset switches off the antenna field for the specified duration. All tags need a certain amount of time to initialize before a command can be processed. The second byte specifies the field recovery time.

Command

Command	Data
'y'	Off time in milliseconds (1 byte) Field recovery time in milliseconds (1 byte)

Answer

Answer	Description
'Y'	After the field reset the reader sends back a 'Y' to acknowledge the command.

© 2008 HID Global Corporation. All rights reserved.

4.3.25 ISO 14443 Type A (MIFARE®) only commands

4.3.25.1 Increment value block (credit)

Increments a value block with a defined value. A read is done automatically after a write to verify data integrity. The command fails if the source block is not in value block format. A previous login is needed to access a block.

Command

Command	Data
'+'	Block (1 byte) Value (4 bytes)

Answer

Answer	Description
Data	Value (4 bytes)
'I'	Error: value block failure
'F'	Error: increment failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
+0400000001	Adds 1 to value block 4
+0500000100	Adds 256 to value block 5

4.3.25.1.1 No value block 'I'

Specified block does not match the value format. The value block is corrupted. A backup block can be used to restore the correct value.

4.3.25.1.2 Increment failure 'F'

This indicates a general failure during the increment procedure or an inability to read after the write process.

4.3.25.1.3 No tag error 'N'

The reader does not detect a response from the tag. There is either no tag present or the tag does not respond to the request.

4.3.25.1.4 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

© 2008 HID Global Corporation. All rights reserved.

4.3.25.2 Decrement value block (debit)

Decrements a value block with a defined value. A read is done automatically after the write to verify data integrity. The command fails if the source block is not in value block format. A previous login is needed to access a block.

Command

Command	Data
'-'	Block (1 byte) Value (4 bytes)

Answer

Answer	Description
Data	Value (4 bytes)
'I'	Error: value block failure
'F'	Error: decrement failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
-0400000001	Subtract 1 to value block 4
-0500000100	Subtract 256 to value block 5

4.3.25.2.1 No value block 'I'

Specified block does not match the value format. The value block is corrupted. A backup block can be used to restore the correct value.

4.3.25.2.2 Decrement failure 'F'

The Decrement failure indicates a general failure during the decrement procedure or inability to read after the write process.

4.3.25.2.3 No tag error 'N'

The reader does not detect a response from the tag. There is either no tag present or the tag does not respond to the request.

4.3.25.2.4 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

© 2008 HID Global Corporation. All rights reserved.

4.3.25.3 Copy value block (backup)

Copies a value block to another block of the same sector. A read is done automatically after the write to ensure data integrity. Used for backup and error recovery. A previous login is needed to access a block.

Command

Command	Data
'='	Source block (1 byte) Target block (1 byte)

Answer

Answer	Description
Data	New value of target block (4 bytes).
'I'	Error: value block failure
'F'	Error: copy failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
=0405	Copy value block 4 to block 5
=0506	Copy value block 5 to block 6

4.3.25.3.1 Target block

The target block does not need to be a valid value block. If the source block is not in value format, the command fails.

4.3.25.3.2 No value block 'I'

Source value block is not in a valid value block. The value block is corrupted. A backup block can be used to restore the correct value.

4.3.25.3.3 Copy failure 'F'

The Copy failure indicates a general failure during the copy procedure or inability to read after the write process.

4.3.25.3.4 No tag error 'N'

The reader does not detect a response of the tag. There is either no tag present or the tag does not respond to the request.

4.3.25.3.5 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

© 2008 HID Global Corporation. All rights reserved.

4.3.25.4 Login (authenticate tag)

Performs an authentication in order to access one sector of a MIFARE® card. Only one sector can be accessed at a time.

Optionally, the command can be used to transmit the key data to the reader-stored keys, in the reader EEPROM.

To store keys in the EEPROM, the write master key command is used. It is possible to store up to 32 master keys in the reader EEPROM. The login requires a successful select.

Command

Command	Data
'l'	Sector (1 byte), valid range 00h - 3Fh Key type (1 byte) AAh authenticate with key type A FFh authenticate with key type A, transport key FFFFFFFFFFFFh BBh authenticate with key type B 10h … 2Fh authenticate with key type A using stored key (00h … 1Fh) 30h … 4Fh authenticate with key type B using stored key (00h … 1Fh) Key (6 bytes) / <CR> (1 byte), optional By transmitting <CR> instead of the key data authentication is done with manufacturer's transport keys (A0A1A2A3A4A5h, B0B1B2B3B4B5h, FFFFFFFFFFFFh).

Answer

Answer	Description
data	Login status (1 byte)
'L'	Login success
'F'	Error: General failure
'N'	Error: No tag
'O'	Error: Operation mode failure
'R'	Error: Out of range
'X'	Error: Authentication failed

© 2008 HID Global Corporation. All rights reserved.

Example

Command	Description
l02AA<CR>	Authenticate for sector 2, using the transport key A (A0A1A2A3A4A5h, key type A)
l3FBB<CR>	Authenticate for sector 63, using the transport key 2 (B0B1B2B3B4B5h, key type B)
l04FF<CR>	Authenticate for sector 4, using the transport key 3 (FFFFFFFFFFFFh, key type A)
l0FAAFFFFFFFFFFFF	Authenticate for sector 15, using key FFFFFFFFFFFFh, key type A
l0E14	Authenticate for sector 14, using EEPROM key 4, key type A
l0530	Authenticate for sector 5, using EEPROM key 0, key type B
l0732	Authenticate for sector 7, using EEPROM key 2, key type B
l0110	Authenticate for sector 1, using EEPROM key 0, key type A
l0ABBFF12FFFFFF35	Authenticate for sector 10, using key FF12FFFFFF35h, key type B

4.3.25.4.1 No tag error 'N'

The reader does not detect a response from the tag. There is either no tag present or the tag does not respond to the request.

4.3.25.4.2 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

4.3.25.4.3 Out of range failure 'R'

The entered key type or the sector is out of range.

4.3.25.4.4 <CR>

Three transport keys are implemented to access cards quickly.

By transmitting <CR> instead of the key, the reader module uses the transport keys for the login procedure.

Command	Description
LxxAA<CR>	Authenticate for sector xx, using the transport key 1 (A0A1A2A3A4A5h, key type A)
LxxBB<CR>	Authenticate for sector xx, using the transport key 2 (B0B1B2B3B4B5h, key type B)
LxxFF<CR>	Authenticate for sector xx, using the transport key 3 (FFFFFFFFFFFFh, key type A)

4.3.25.4.5 Login with key data from EEPROM

Each key stored in the reader EEPROM can be used as type A or type B key. To use a key as type A, the value 10h must be added to the key index. 30h must be added to use a key as type B.

© 2008 HID Global Corporation. All rights reserved.

4.3.25.4.6 Usage of key A, key B

MIFARE® cards support two different crypto keys for each sector. Each key is 32 bits long and is stored in the sector trailer (last block of the sector) on the card. It is possible to set different access rights for each key.

4.3.25.5 Read value block

Reads a value block. The command checks if data is in value block format. The read value block command needs a successful login.

Command

Command	Data
'rv'	Value block (1 byte)

Answer

Answer	Description
Data	Read value (4 bytes)
'F'	Error: General failure
'I'	Error: value block failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
rv04	Reads value of block 4.

4.3.25.5.1 No value block 'I'

The value read back after the write value command is not a value block. Data was written corruptly.

4.3.25.5.2 No tag error 'N'

This means that the tag does not respond, because either there is no tag present or none of the tags in the field are authenticated ('I' instruction).

4.3.25.5.3 General failure 'F'

In addition to the case of a data read failure caused by bad transmission conditions, this error is returned if a sector is addressed which is not located in the authenticated area.

4.3.25.5.4 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

© 2008 HID Global Corporation. All rights reserved.

4.3.25.6 Write value block

This command formats a block as a value block containing a 32-bit value. A read is performed automatically after the write. Value blocks need a complete 16-byte block due to redundant storage. A successful login is required to run the command.

Command

Command	Data
'wv'	Value block (1 byte) Value (4 bytes)

Answer

Answer	Description
Data	Written value (4 bytes)
'I'	Error: value block failure
'F'	Error: write failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
wv05010055EF	Writes value 010055EFh to block 5.

4.3.25.6.1 Invalid value 'I'

The value read back after the write value command is not a value block. Data was written corruptly.

4.3.25.6.2 Write failure 'F'

In addition to the case of a data read failure caused by bad transmission conditions, this error is returned if a sector is addressed which is not located in the authenticated area.

4.3.25.6.3 No tag error 'N'

This error is returned if no tag is present or the card does not respond.

4.3.25.6.4 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

4.3.25.6.5 Writing values

The write value block command is designed to create blocks in value format. This command requires write access to the specified block. Using this instruction for ticketing operations is not recommended. For ticketing applications, special instructions (Increment/Decrement/Copy) are available.

© 2008 HID Global Corporation. All rights reserved.

4.3.26 SR176 only commands

4.3.26.1 Lock block

This command locks a block permanently.

Command

Command	Data
'k'	Block address (1 byte)

Answer

Answer	Description
data	'K' + page address
'F'	Error: Lock failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure (only SR176 tags supported)
'X'	Error: Block already locked

Example

Command	Description
k05	K05 Lock block 05.

4.3.26.1.1 Operation mode failure 'O'

The presented tag is not a SR176 tag.

4.3.26.1.2 Apply settings

After locking a block permanently, the tag needs to be selected for the settings to apply.

© 2008 HID Global Corporation. All rights reserved.

5 Frequently Asked Questions

5.1.1 Getting Started

To test and interface the Dual ISO Module, you do not need a sophisticated µP development system. All you need is a PC, a connection cable and a power supply for the reader. If you are using Microsoft Windows (95/98/NT/…), take the following steps:

- Make sure, that your reader has an RS232 interface
- Start HyperTerminal
- Create a new connection (FILE/NEW CONNECTION)
- Enter a name for the connection (i.e. 'MIFARE')
- Select connect COM2 (COM1) direct connection
- Connection setup 9600, 8, n, 1, no handshake
- Connect your reader to COM2 (COM1) of the PC and apply appropriate supply voltage. The reader transmits a string ("Dual 2.2") to the PC.
- This string denotes the firmware provided with your reader module
- Put a tag to your reader. Serial numbers should be displayed properly
- Enter commands via keyboard. They should be transmitted to the reader and the reader should reply

If using an operating system different from Microsoft Windows, you may use any other terminal program that is capable of receiving/transmitting data via the serial port of your PC.

5.1.2 How should the Dual ISO Reader be personalized?

In ASCII protocol applications, no personalization is necessary.

In applications that are using the binary protocol mode, personalization is required. Use the Utility program to set up your reader correctly. Ask the reseller or the HID ID sales representative for the Utility software or download it from http://www.hidglobal.com/omnikey. Minimum requirements are WIN98SE, WIN 2000, WIN XP and a free COM port on the PC.

5.1.3 What type of MIFARE® card should I use?

The MIFARE® standard is designed for multi-application environments. It contains 16 sectors each with 2 individual keys, access conditions, and 3 data or value blocks. Some applications use the 1 Kbytes of the MIFARE® Standard Card Memory only as storage area.

MIFARE® Ultra light has no crypto unit on chip. It only supports 16 blocks.

MIFARE® Standard 4k cards have the same features as MIFARE® Standard cards but increased memory capacity.

© 2008 HID Global Corporation. All rights reserved.

5.1.4 How safe is MIFARE® Standard for cashless payment?

Security is always a feature of the overall system, not of the components. It requires careful design.

A properly designed system will require **ALL** barriers to be hacked in order to be broken.

For good design start identifying possible attacks and then create barriers to block them.

MIFARE® was specifically designed for cashless payment applications. The MIFARE® concept provides the following security barriers:

- Anti-collision/-selection
- Atomic value transaction
- Ciphered communication
- Storage of values and data protected by mutual authentication
- Weak field keys that allow decrement only
- Stored keys in the reader that are not readable
- Keys in the card that are not readable
- A brute force attack based on trying many different keys is limited by the transaction time (several ms) of the card and would last virtually forever.

The Application can and should provide more barriers:

- Sector access conditions. It is possible to assign access conditions in a way that only decrementing of values is allowed with the keys used in the field. So even a manipulated field station cannot be used to increment the value on the cards. As a general rule, key A is used as a field key, allowing only to read and decrement values, and key B is used to format the card or increment values.
- Diversified keys. To make life even harder for attackers, keys can be modified using the serial number and memory content of the card. So each card uses different keys and a listening attack on the reader interface would be hopeless.
- Limiting cash volume stored on a card
- Do not use the transport keys (keys programmed at the time of delivery) for ticketing applications!
- Ciphered and scrambled data storage
- Sabotage alarm
- Even higher security with contact less controller cards like DESFire, MIFARE® ProX, MIFARE® Smart MX etc.

© 2008 HID Global Corporation. All rights reserved.

5.1.5 Using a MIFARE® card

This example demonstrates the detection of a card in the antenna field with continuous read and the reading of a page.

Table 31 Using a MIFARE® card

Command	Answer
c	Activate continuous read mode
	B2197B58 a card responds with its serial number
.	S abort continuous read mode
s	B2197B58 select card
l01AAFFFFFFFFFFFF	L login into sector 1 with key FFFFFFFFFFFFh key type A
rb04	00112233445566778899AABBCCDDEEFF read block 04
c	Activate continuous read mode to detect a new card

5.2 Using a DESFire card

5.2.1 Create a plain standard data file

After activation, application 0 is selected automatically. Default access rights of application 0 require a login to create an application. The following example illustrates the successful creation of a plain standard data file.

Command	Answer
s	04E10E00000000 activate card
f1200000000000000000000000000000 0000000000	L login to application 0
f06050000100F01	00 create application with ID 000010
f0408000010	00 select application with ID 000010
f080F0000eeee10000000	00 create plain standard data file with ID 00

© 2008 HID Global Corporation. All rights reserved.

5.2.2 Use a plain standard data file

The next example demonstrates the use of a plain standard data file, such as that created in the previous example. No login needed since the file is plain.

Command	Answer
s	04E10E00000000 activate card
f0408000010	00 select application with ID 000010
f020D00	00 select file with ID 00
f09160000001122334455	00 write data to standard data file
f051500000010	00112233445500000000000000000000 read data from standard data file

5.2.3 Use a DES secured value file

The next example demonstrates the use of a DES secured value file, such as the one created in the previous example. After the selection of the application, a login with the key of the value file is needed to access the file. Modification of the value file is accepted after the commit transaction command is given.

Command	Answer
s	04E10E00000000 activate card
f0408000011	00 select application with ID 000010
f03000000	L login to application
f020D00	02 select file with ID 00 (value file)
f0117	0055555555 read value file data
f051911111111	00 debit value file with 11111111
f0117	0055555555 read value file, no modification done
f011c	00 commit transaction, modification is done
f0117	0044444444 read value file, verify modification

© 2008 HID Global Corporation. All rights reserved.

References

[1] ISO/IEC 14443 Part 1-4, Identification Cards – Contact less integrated circuit(s) cards – Proximity cards

[2] DESFire Documentation, Philips, http://www.semiconductors.philips.com

[3] Data Encryption Standard (DES), FIPS PUB 46-3,
Reaffirmed 1995 October 25

[4] HID Antenna Design Guide

[5] Philips; Application Note, MIFARE® & I-Code, Micore Reader IC family Directly Matched Antenna Design

Appendix A – Antenna

According to antenna design, please refer to the Philips Application Note (MIFARE ® & I-Code, Micore Reader IC family Directly Matched Antenna Design) or to the HID GLOBAL Antenna Design Guide.

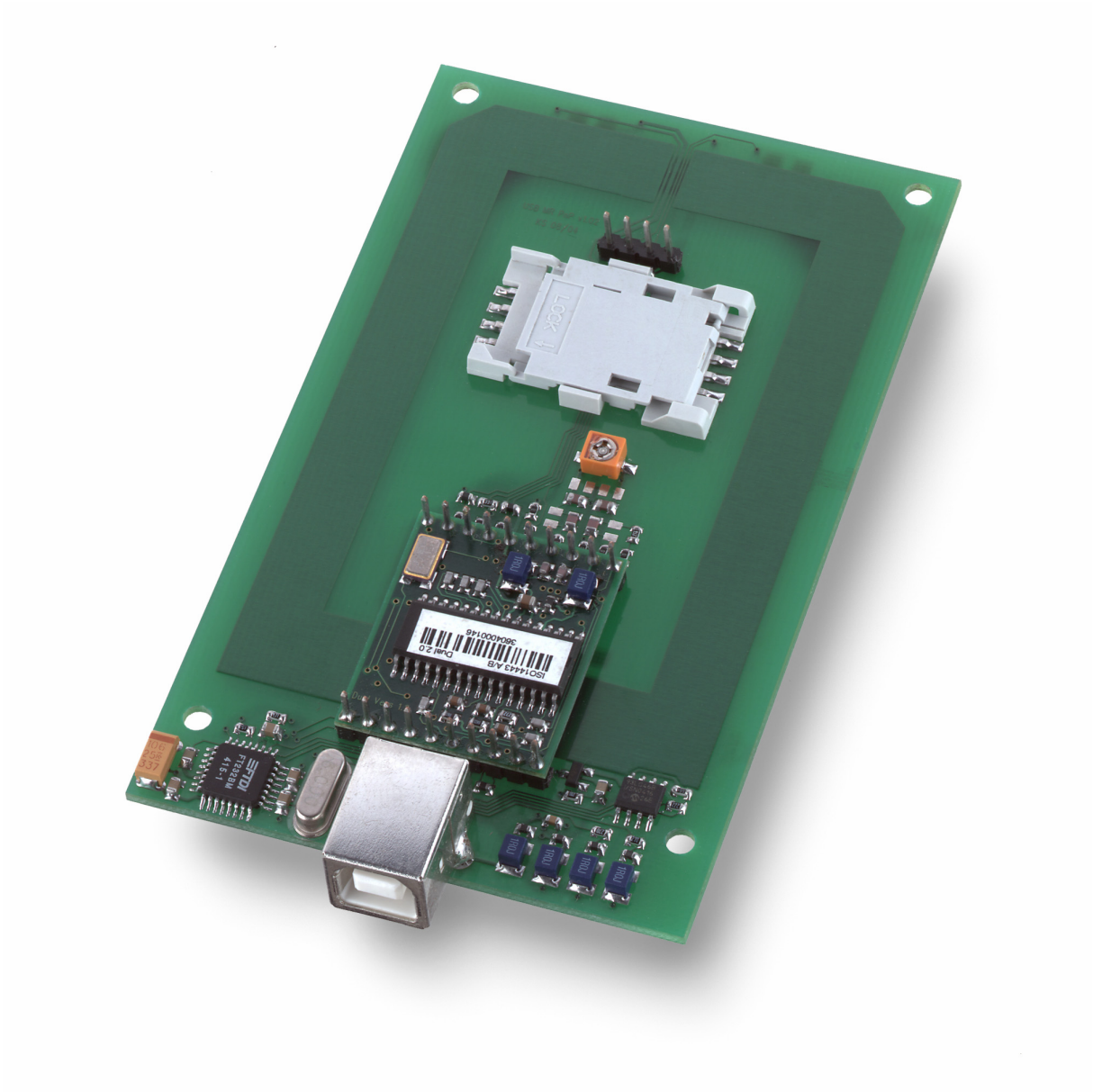
Appendix B – SAM

Please note that the power supply of the SAM adapter must be turned off during the entire card insertion period, otherwise SAM card damage might occur.

For proper usage of the SAM, a 100nF capacitor between V_{cc} and GND is necessary.

© 2008 HID Global Corporation. All rights reserved.

Appendix C - Short Range Plug & Play Module (RDHS-0404N0-03)

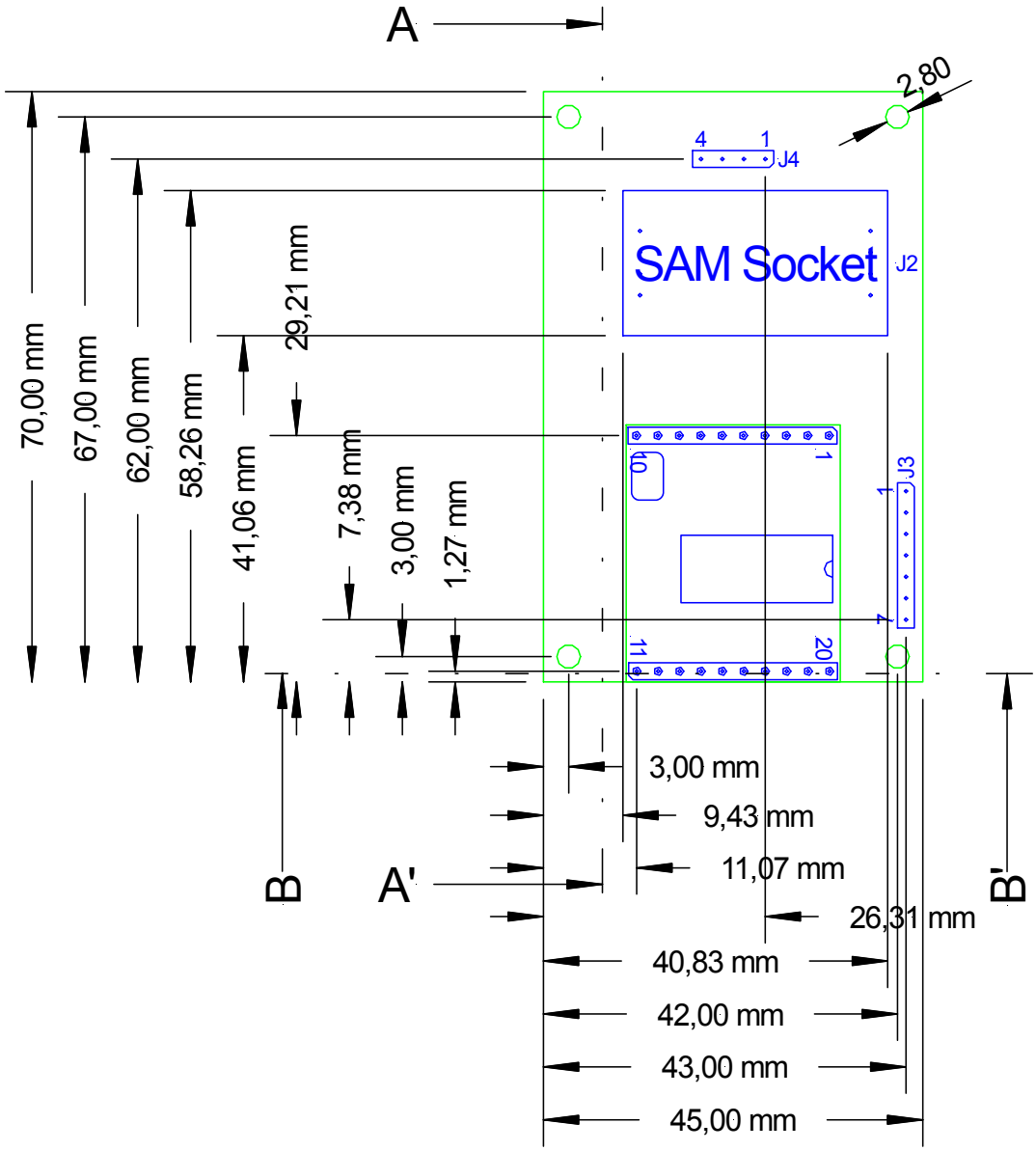


© 2008 HID Global Corporation. All rights reserved.

Dimensions

Top view

All dimensions are listed in mm



© 2008 HID Global Corporation. All rights reserved.

Appendix D - Timings

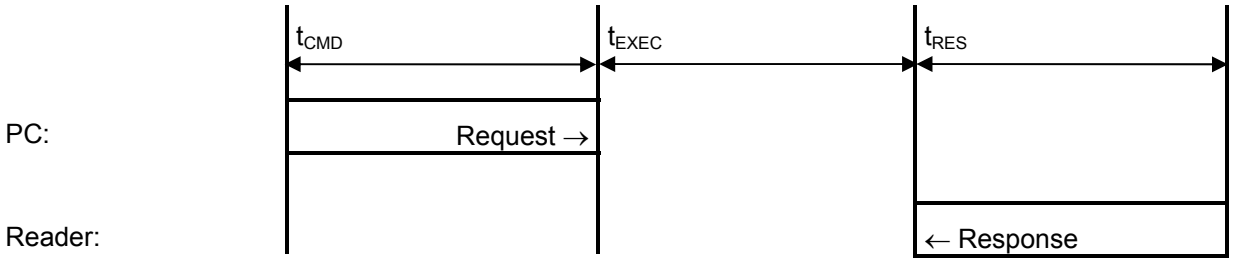


Table 32 Timings

Command	t_{EXEC} [ms]	Comments
Common commands		
Cont. read (locked tag)	2.8 – 22.6	+ Reset Off and Recovery Time
Cont. read (worst case)	54	+ 3x Reset Off and Recovery Time
DES en/decryption	9.6 – 9.7	
TDES en/decryption	28.7 – 28.8	
High-speed select 'h08' (locked tag)	8.9 – 14.4	+ Reset Off and Recovery Time + SFGT
High-speed select 'h08' (no tag)	15	+ 3x Reset Off and Recovery Time
High-speed select 'h08' (worst case)	14.7	+ 3x Reset Off and Recovery Time + SFGT
Multi-select (locked tag)	5.8 – 11.4	+ Reset Off and Recovery Time
Multi-select (no tag)	67	+ Reset Off and Recovery Time
Multi-select (worst case)	67	+ Reset Off and Recovery Time
Antenna on	0.2	+ Reset Recovery Time
Antenna off	0.2	
Port read	0.1	
Port write	0.1	
Read block	1.8 – 2.2	
Write block	8.2 – 11	
Reset	13.2	
Select (locked tag)	5.4 – 22.8	+ Reset Off and Recovery Time
Select (no tag)	38	+ 3x Reset Off and Recovery Time
Select (worst case)	55	+ 3x Reset Off and Recovery Time
ISO 14443 Type A only commands		
Increment value block	18.4	
Decrement value block	18.4	

© 2008 HID Global Corporation. All rights reserved.

Command	t_{EXEC} [ms]	Comments
Copy value block	18.5	
Read value block	2.3	
Write value block	7.9 - 10.5	
MIFARE® Login	4.9	
Power conditions		
Power on	79	Does not include rise time of power supply
Enable on	85	

Default Command Guard Time (20h = 1.2ms) was used.

All timing data is advisory application information and does not form part of the specifications. It may change in future firmware releases. Please also note that all values specified in the above table depend on the tag used and Command Guard Time.

© 2008 HID Global Corporation. All rights reserved.

Appendix E - Release Notes

5.3 Version History

Date	Revision number
10/27/2008	**Version 2.4 Rev 2.0** HID Format
8/07/2007	Version 2.4, Rev. 1.0
08/01/2005	Version 2.2, Rev. 1.1 Tag type for cascade level corrected SAM internal pull-up corrected to 3.3kΩ
05/17/2005	Version 2.2, Rev. 1.0
02/18/2005	Version 2.1, Rev. 1.0

5.3.1 Dual 2.4

- Extended ID supports the ISO 14443 A SAK byte
- High Level support of the Innovision Jewel tag (selection, read and write operations)
- Added functionality to switch between ReqA/B or WupA/B usage
- The Quiet command no supports ISO 14443 part 3 and 4.
- Improved ISO 14443 4 handling
- Changed LED behavior in continuous read mode and multilist
- Increased LED flash duration time
- New command "ox" added to reread all register settings

5.3.2 Dual 2.3

- Master clear pin added (MCLR): resets the register values to default
- Resend last answer command added
- Support of asynchronous baud rates for the high speed select command
- Register default value changed for Selection Timeout ISO 14443 B
- Added commands to read and write multiple blocks (‘rd’ / ‘wd’)
- Flag added to disable read after write
- Bug fixes

5.3.3 Dual 2.2

- Sending serial data frames over User Port
- Automatic ISO 14443-4 timeouts can be switched on/off
- Request A information within ISO 14443 A Extended ID answer can be switched on / off
- Command Guard Time added
- 'of' and 'og' commands get new parameters

© 2008 HID Global Corporation. All rights reserved.

- Chaining of 256 byte frame support
- Support of ASK GTML tag
- Page read functionality added
- Additional protocol register PCON3
- Some bug fixes

5.3.4 Dual 2.1

- High-speed select supports anti-collision and the forcing of the air interface transmission rate and the frame size
- Automatic ISO 14443-4 error handling (can be switched on/off)
- RATS answer is returned with high-speed select command for ISO14443 A tags and with Extended ID flag set
- Support for the ISO14443 B anti-collision algorithm
- Extended Protocol flag now switches on/off, complete ISO14443-4 handling
- ISO14443-4 chaining and WTX improved
- 'of' and 'og' commands get new parameters
- Selection time-out for ISO14443-4 A tags is set to 10h

5.3.5 Dual 2.0

Initial Release

© 2008 HID Global Corporation. All rights reserved.

Appendix F - Approvals / Certificates

CE Declaration

The HID GLOBAL HF Dual ISO Reader Module complies with the European CE requirements specified in the EMC Directive 89/336/EEC.

If the HID GLOBAL HF Dual ISO Reader Module is operated with other components, all power connections and additional components of the final device must comply with the European EMC directive.

Additional connections may have a length of up to 2 m maximum, or in fixed installations up to 1 m maximum.

European customers must themselves make sure that the final device conforms to the European EMC Directive.

MIFARE Certificate

The HID Global HF Dual ISO USB Plug & Play Board and the HID Global HF Dual ISO USB Desktop Unit comply with the Philips MIFARE requirements. The units have shown their compliance during extensive tests at the Arsenal Research Institute, located in Vienna/Austria. Arsenal Research is the official MIFARE certification institute.

© 2008 HID Global Corporation. All rights reserved.